



SOUNDSENTRY™ SECURE MEETING ROOM SOLUTIONS

A COMPREHENSIVE SOLUTION FOR
EFFECTIVELY CONDUCTING SENSITIVE
MEETINGS WITHOUT THE RISKS OF
EAVESDROPPING AND DATA BREACHES

INTRODUCING **SOUNDSENTRY™**

The SoundSentry family is a comprehensive solution for conducting classified and unclassified meetings using the same room, with no risk of data leakage.

It is the world's only solution specifically designed to protect classified & sensitive information through a three-layered approach:

SECURE PERIPHERAL SHARING -

Share a single set of peripherals across multiple air-gapped networks and classification levels. HSL's NIAP-certified KVMs enforce absolute data isolation, making data leakage between sources impossible.

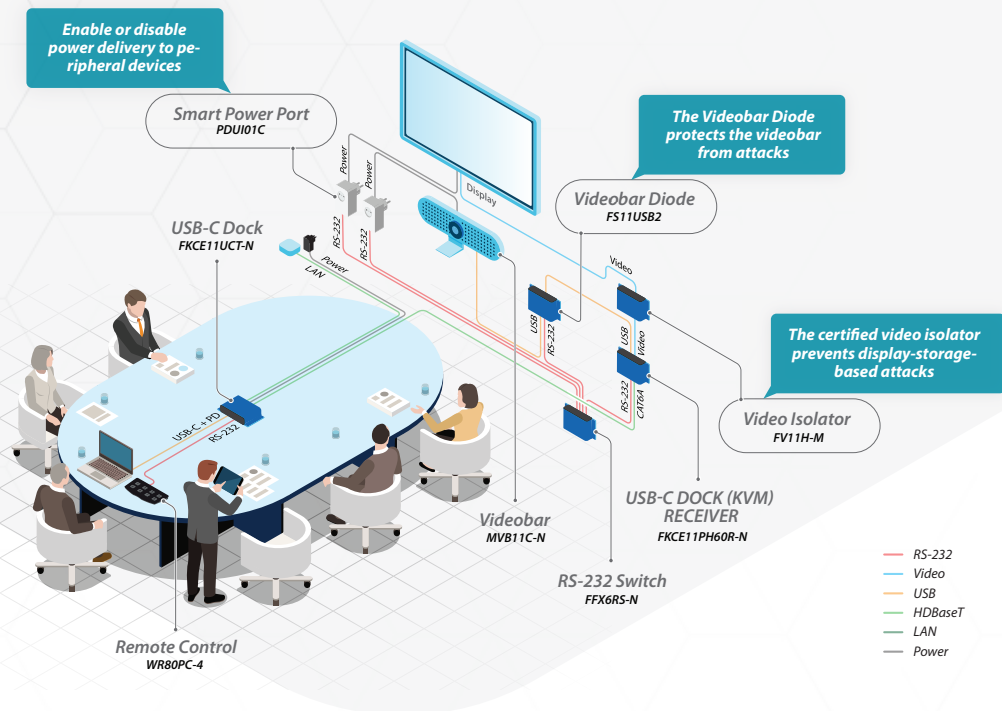
COMPREHENSIVE VIDEO AND AUDIO DIODES -

Eliminate hardware-level data breaches with HSL's media diodes. These create a physically enforced, unidirectional data path, making it impossible for data to leak back from a media device to the source computer.

SMART POWER MANAGEMENT -

Instantly harden meeting room security by cutting power to vulnerable peripherals like displays and videobars. This offers a true hardware disconnect, a level of security that simply muting a device cannot provide.





PROTECT ANY MEETING

Hardware-based security provides the definitive form of protection by physically eliminating vulnerabilities at their source.

The specific SoundSentry configuration is selected to match the room's unique requirements - including size, participant count, and purpose - accounting for all associated threats and meeting requirements.

To see examples of various room configurations, visit the SoundSentry solution page:



THE SOUNDSENTRY™

FAMILY OF SECURE PRODUCTS



VIDEOBAR

A wired-only design to eliminate wireless threats, volatile memory with no battery backup that erases all data on power off, and tamper-proof firmware.



MINI-MATRIX / ULTRA MINI-MATRIX

Securely interact with multiple computers with one keyboard, mouse, and dual 4K monitors. NIAP PP4.0 certified for maximum security.

VIDEOBAR DIODES

Creates a one-way, filtered path for A/V only, isolating the videobar from all network devices and blocking any non-media data. Safely share a videobar among multiple computer sources.



ACTIVE QUIET BOX

Blocks smartphone microphones from capturing or transmitting audio.



SMART POWER PORT

Enable/disable power delivery to conferencing devices through remote controls.



TAA\BAA USB-C DESKTOP DOCKING SOLUTIONS

Connect peripherals locally or at a distance. USB-C docking stations and extenders provide flexible setups, supporting peripheral access at up to 100m.

REMOTE CONTROLS

Instantly switch between security presets, manage input sources, and configure multiview layouts.



RS-232 SWITCH

Allows a single remote control to manage multiple RS-232 devices.



NIAP CERTIFIED VIDEO ISOLATORS

Enforce a unidirectional data flow from the computer to peripherals, eliminating threats from compromised devices.



TYPICAL MEETING ROOMS

VULNERABILITIES

The convergence of networks, guest devices, and intelligent AV technology makes the modern meeting room a prime target for cyber threats. Each connection point is a potential vector for malware, every remote session is a risk for interception, and every piece of hardware is a potential attack surface.



NETWORK INFILTRATION

Compromised guest devices gain direct access to secure organizational networks by exploiting KVM switch and peripheral device vulnerabilities.



PERIPHERAL DEVICE EXPLOITATION

Microphones, speakers, displays and cameras can be exploited for persistent eavesdropping, malicious code injection and data exfiltration.



ACOUSTIC HACKING

Speakers transmit undetected high-frequency audio signals to exfiltrate data.



SECURITY FEATURES

- Audio stream is protected by a low-pass filter preventing high frequency data breaches.
- Unidirectional data flow prevents data breaches through peripheral devices and the retasking of audio speakers as microphones. Optical data diodes prevent mixing data between sources, including guest computers.
- Immune to wireless hacking attempts.
- No back-up batteries – information cannot be stored in a device for delayed exfiltration.
- Normally closed Videobar Diode prevents inadvertent audio and video transmissions.
- Remote controlled Smart Power Port cuts power to the Videobar, display and Videobar Diode, depending on the classification level of the meeting.
- Smartphone eavesdropping prevention through anechoic isolation and active noise obfuscation.
- Anti-tamper mechanism and holographic anti-tamper labels.
- TAA & BAA compliant secure supply chain and manufacturing prevent zero-day supply chain attacks.

HIGH SEC LABS (HSL)

DEVELOPS HIGH-QUALITY CYBER-DEFENSE SOLUTIONS FOR PROTECTING NATIONAL ASSETS AND INFRASTRUCTURE IN THE FIELD OF NETWORK AND PERIPHERAL ISOLATION.



www.highseclabs.com

© 2025 HighSecLabs Inc. All rights reserved. HSL logo and product names are trademarks or service trademarks of HighSecLabs Ltd (HSL). All other marks are the property of their respective owners. Images for demonstration purposes only. Patents: www.highseclabs.com/patents/. HLT35572 Rev 1.1