SOUNDSENTRY™

SECURE MEETING ROOM SOLUTIONS

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

HighSecLabs
Highest Security Solutions

INTRODUCING
SOUNDSENTRY™

The SoundSentry solution family protects sensitive meetings from cyber threats while streamlining conferencing functionality in secure, multi-domain environments. To meet varying security needs and room sizes, SoundSentry is built on a three-layered security approach:

SECURE PERIPHERAL SHARING -

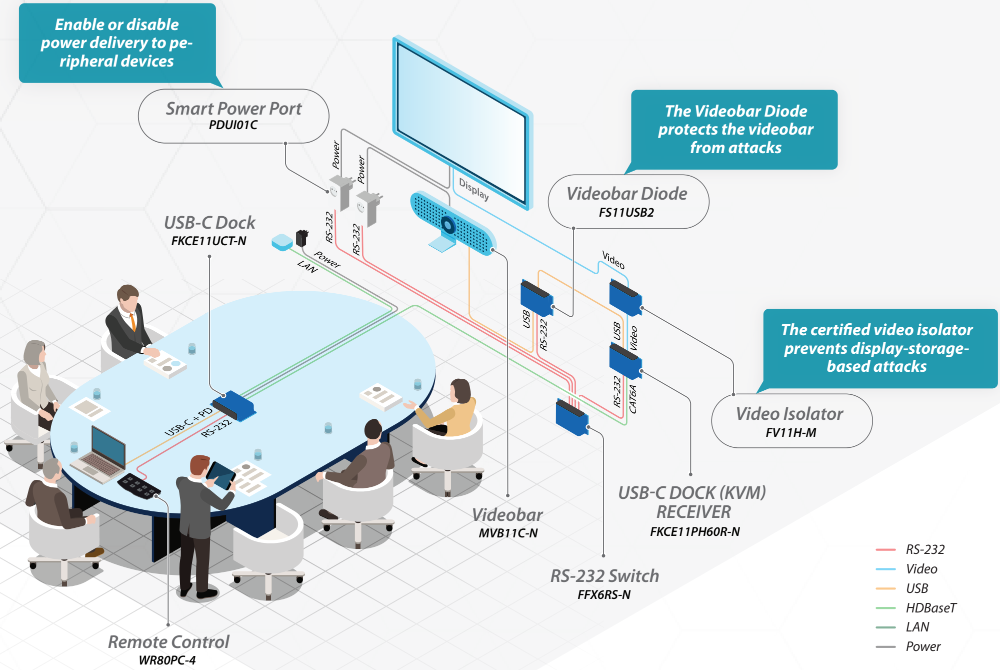
Control multiple devices from a single console without the risk of data leakage. HSL's NIAP-certified KVMs enforce absolute data isolation between each connected device, ensuring one network cannot compromise another.

COMPREHENSIVE VIDEO AND AUDIO DIODES -

Eliminate data exfiltration at the hardware level. Our solutions create a physically enforced, one-way data path—using only wired connections—making it impossible for data to leak between networks through vulnerable peripheral exploitations.

SMART POWER MANAGEMENT -

Instantly match room security to meeting sensitivity by switching from a fully operational 'Standard Mode' to a 'Secure Mode' that physically cuts all power to high-risk peripherals like displays and videobars. This provides absolute, hardware-level certainty that they are completely off, eliminating any risk of eavesdropping or data breaches.



Enable or disable power delivery to peripheral devices

The Videobar Diode protects the videobar from attacks

The certified video isolator prevents display-storage-based attacks

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.

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.

SMART POWER PORT

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

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.

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.

ACTIVE QUIET BOX

Blocks smartphone microphones from capturing or transmitting audio.

DOCKING STATIONS & EXTENDERS

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

SECURE 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.

NIAP®

TRADE AGREEMENTS ACT TAA COMPLIANT

BAA COMPLIANT

www.highseclabs.com