HSL Company Profile

HighSecLabs
Highest Security Solutions Ltd.

High Sec Labs Profile

- Privately-owned, HQ in Israel
- Founded in 2008
- Locations in Israel and the USA, 300 employees, 100 R&D Positions
- HSL holds all development expertise internally (HW, FW, Mechanical design)
- Secure Manufacturing facilities in Israel and the US
- X-ray and AOI machines in house
- Main Markets: US, Canada, Europe
- Multiple international certifications - NIAP/Common Criteria
- IP – 70 patents granted, dozens more submitted

High Sec Labs – Field of Operation

High Sec Labs (**HSL**) creates cyber security solutions for organizations with multiple isolated networks.

HSL is primarily a HW development company which relies on physics to create cyber security solutions rather than logic.

HSL operates in multiple international markets and has experience developing products and analyzing 3rd party solutions to achieve the highest possible level of security for its customers.

HSL has membership on multiple international standards boards and develops products to meet and exceed international requirements.

HighSecLabs
Highest Security Solutions Ltd.

High Sec Labs – Products Portfolio

HighSecLabs
Highest Security Solutions Ltd.

TARGET HSL's VERTICALS

Government and National Infrastructure

Banking and Trading

Command & Control

Defense

HighSecLabs
Highest Security Solutions Ltd.

Desktop Security Solutions

HighSecLabs
Highest Security Solutions Ltd.

Secure Desktop Solutions

High Sec Labs (HSL) has created a wide portfolio of products designed to solve cyber security issues originating from the user desktop. **HSL**'s solutions protect against misuse of peripherals to leak information from classified networks to non classified and vice versa.

While airgap is the most effective way to protect against cyber threats in a classified environment, organizations which are choosing this method are creating usability issues for themselves.

HSL's mission is to protect and isolate peripherals and networks while allowing an easy and intuitive user experience in an air gapped environment.

Secure KVM Switches

Audio Diodes

Multi-Domain Readers

USB eLocks

VoIP phones Protection

HighSecLabs
Highest Security Solutions Ltd.

The need for a Secure KVM Solution

When is a *SECURE* KVM Needed?

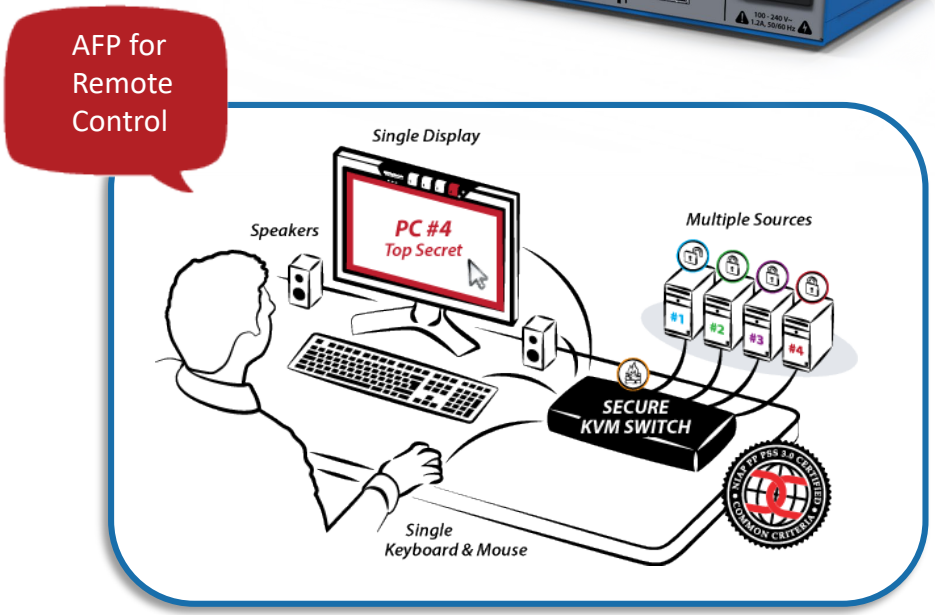
When users who connect multiple computers of different classification networks or to the Internet - through the KVM - they are at risk.

Why? Because most computer peripherals have no security mechanisms whatsoever to assure no data leaks between connected computers.

So, they're subject to data leakage, signaling, and malicious code attacks by hackers.

High Sec Labs has the widest variety of secure KVM switches certified by NIAP according to the latest Protection Profile (PP).

- 2 Ports, 4 Ports and 8 Ports
- Single head and Dual Head
- DVI, DP and HDMI
- 4K 60 HZ
- Unique DP\HDMI joint connectors for easier interoperability of devices
- Unique remote control options

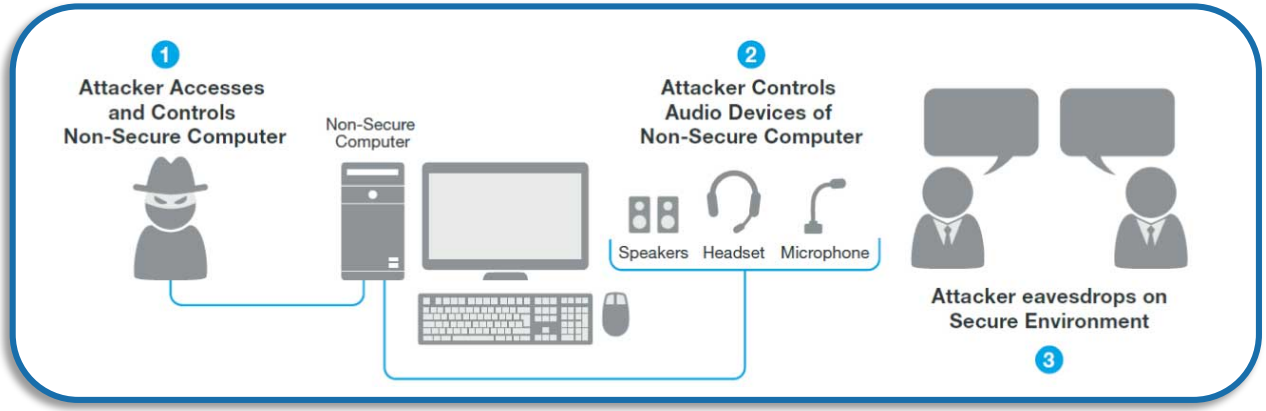


HighSecLabs
Highest Security Solutions Ltd.

Audio Diode Product Line

The Audio Diode mitigates risks of using peripheral audio devices in organizations with multiple isolated networks

- Blocks eavesdropping of surrounding conversations, by forcing unidirectional audio flow.
- Low-Pass Filter - prevents hackers from attacking by broadcasting either high- or low-frequency signals through audio devices
- Effective in classified areas which also have PCs connected to non-classified networks
- Optional speaker and mic enable button to control audio device connection



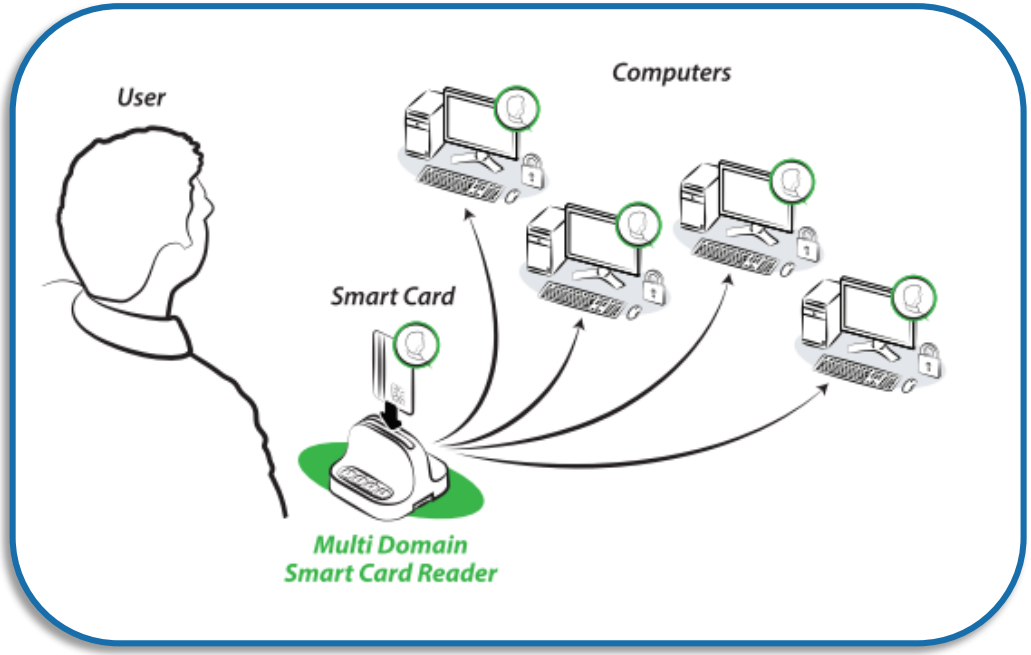
HighSecLabs
Highest Security Solutions Ltd.

MDR – Secure Multi-Domain Smart Card Reader

- Enables a single user smart card to securely logon to two or four isolated computers simultaneously eliminating the need for a separate smart card for each computer
- HSL MDR available in 2 port or 4 port interfaces with 2/4 computers thorough USB cables
- Once the card is pulled out all authentication sessions are immediately disconnected.
- The MDR is fully isolated internally to prevent any potential data leakages between coupled computers through the reader.
- The MDR automatically switches between channels. The user needs minimal training in device operation.
- The MDR reduces overall smart card operational costs and allows simultaneous work on multiple networks.

RS20N-4

RS40N-4



HighSecLabs
Highest Security Solutions Ltd.

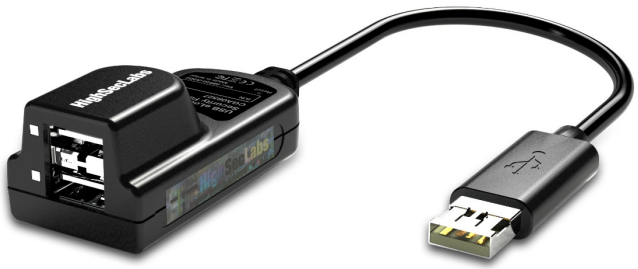
Secure USB Solution

HSL's USB solution blocks all open ports with mechanically locked devices to protect against misuse of the ports for attacks:

- USB Plugs – Mechanical USB plug that physically locks individual USB ports. Forced removal permanently damages the USB port.
- HID Filter – A dongle designed to allow HID devices only
- Configurable Filter – A configurable dongle which can be programed to allow only specific USB devices based on predefined user rules

Hardcoded HID Filter

- Accepts only USB HID Devices (Keyboard/Mice)
- Unidirectional, protected by optical data diodes
- Full HID emulation



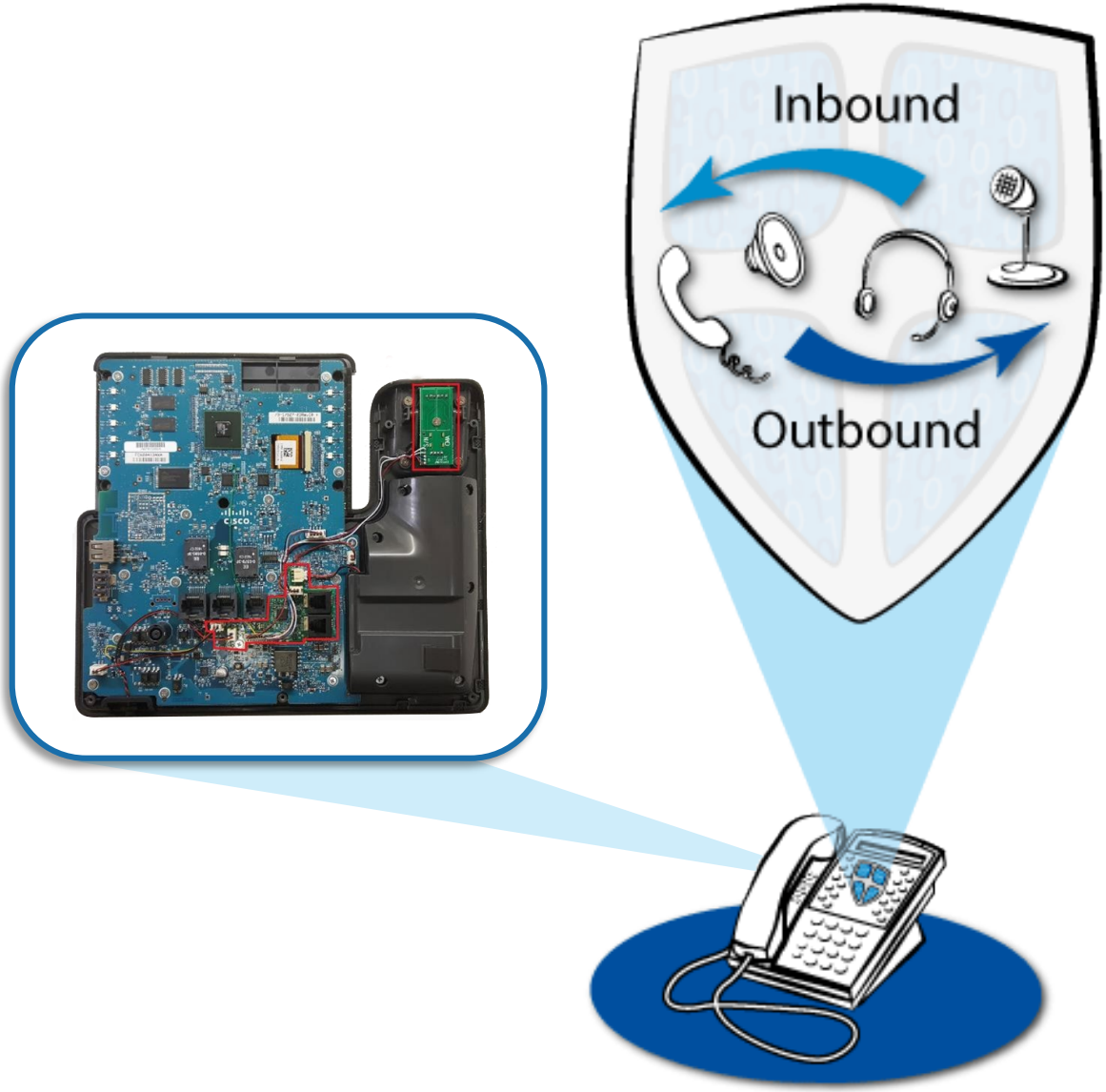
Configurable Filter

- Accept USB devices based on unique identifiers such as Serial/HID/VID/Class ID, etc.
- Configurable identifiers to fit with specific customer peripherals

HighSecLabs
Highest Security Solutions Ltd.

HSL Secure VoIP Implant

- The HSL Secure VoIP Implant is securely embedded inside a standard VoIP telephone.
- It is designed to mitigate eavesdropping and prevent a remote attacker from exploiting the phone to listen to surrounding classified conversations.
- The implant allows normal phone operation without any negative effect on performance or user experience.
- Audio and visual notifications provide clear and simple user indications of the phone's secure state.



Command and Control Solutions

HSL Secure Command and Control Solutions

Command and Control Users (especially in a secure environment) requires a very flexible work environment. They need to view and interact with multiple systems simultaneously.

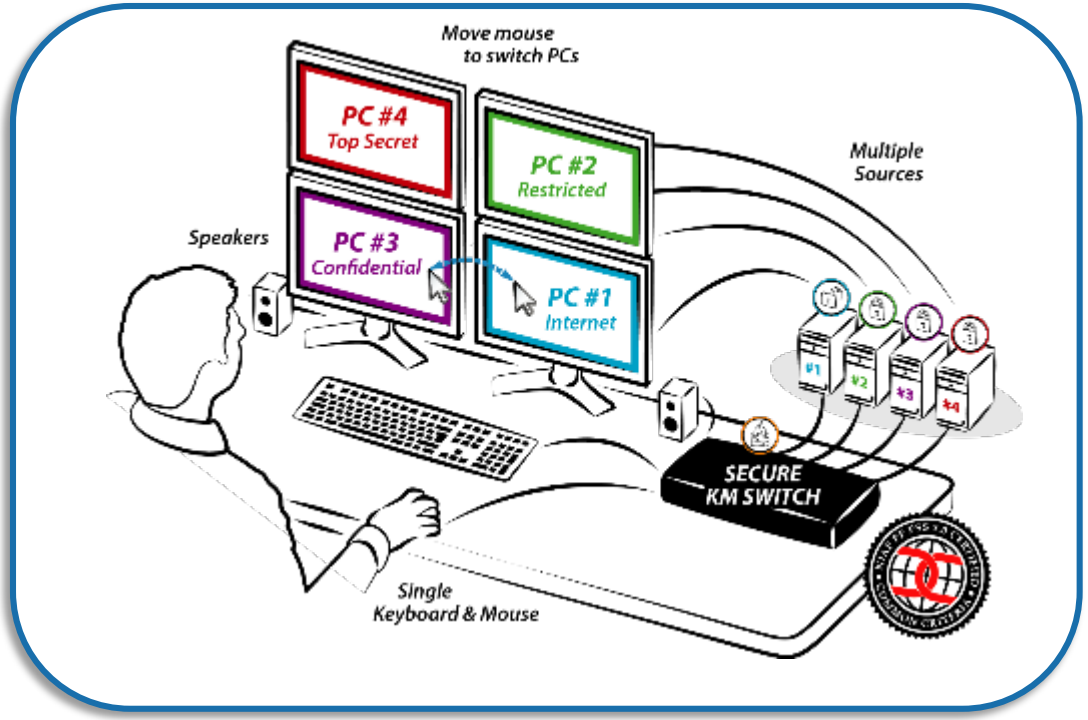
High Sec Labs (HSL) has created several solutions to service these power users while maintaining the required network separation.

HighSecLabs
Highest Security Solutions Ltd.

HSL KM Switches

A KM switch enables users to:

- Work simultaneously with multiple computers connected to multiple displays using one set of audio, keyboard and mouse peripherals
- Interact with multiple computers in real-time while maintaining the highest isolation between computers and peripherals
- Directly connect separate displays to each computer and securely share keyboard, mouse, audio, and USB devices



HSL MINI-MATRIX KVM Switches

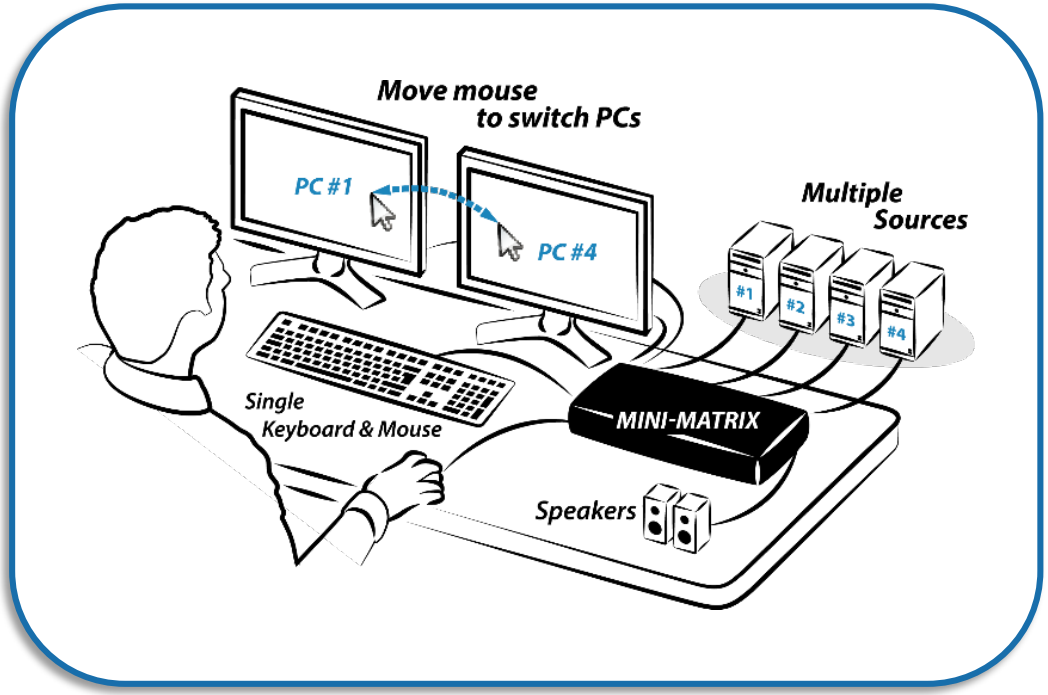
A Mini-Matrix lets users view and control **two** out of all (four or eight) computers – on **two** displays – while sharing a **single** keyboard-and-mouse set.

The Mini-Matrix enables users to both:

- Free up their desktops from the clutter of multiple peripherals
- Access two selected computers simultaneously

A Mini Matrix is ideal for meeting rooms and control centers, where multiple computers have to be presented – at the same time – on two displays. For example:

- In control centers, where information from several sources needs to be constantly displayed in real-time
- In meeting rooms, where both visitor and host computers are viewed and controlled simultaneously



HighSecLabs
Highest Security Solutions Ltd.

New Accessory - AFP

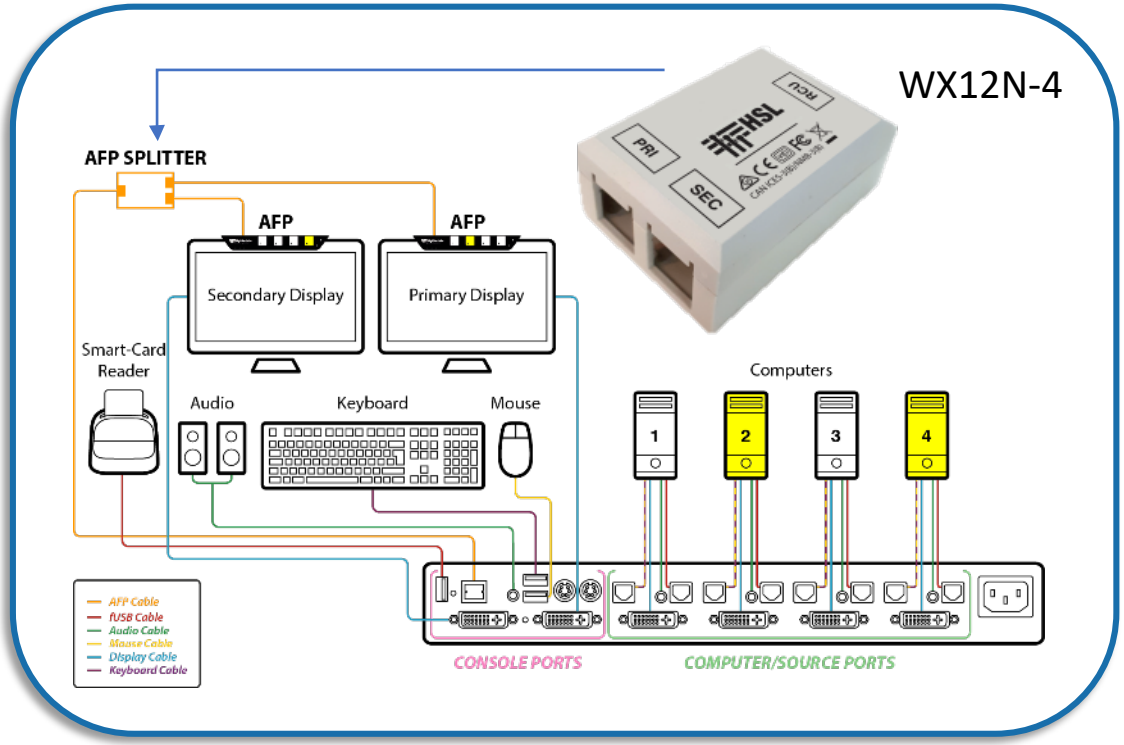
4/8 Port Auxiliary Front Panel

- Remote control for the KVM switch, right from the desktop or monitor
- Simply mounts on a desktop or display
- Push Buttons, like those on the KVM, for easy channel switching, combined with LEDs that show the active PC
- Communicates via a standard RS232 protocol for easy and intuitive control
- Compatible with all 4/8 Port PP3.0 and PP4.0 KM, KVM, and Mini-Matrix switches, as well as PP4 Combiners
- **Matrix AFP Splitter** – This enables attaching an additional AFP to the second monitor connected through the Mini Matrix Switch

WR80

WR40-3

WX12N-4



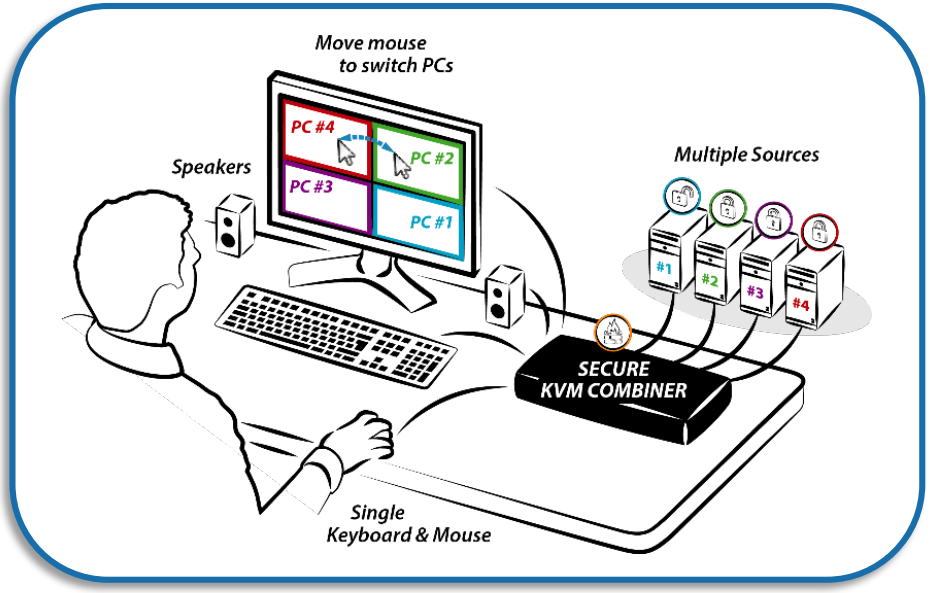
HSL KVM COMBINER

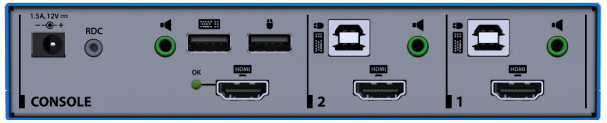
A KVM Combiner is a multi-viewing KVM switch that lets users share a **single** keyboard-and-mouse set, to control:

- **All** connected computers
- On **one** display (or two, in extended-view mode)

This enables users to both:

- Free up their desktops from the clutter of multiple peripherals, especially displays
- View **all** computers in a single glance – for quick and laser-focused control



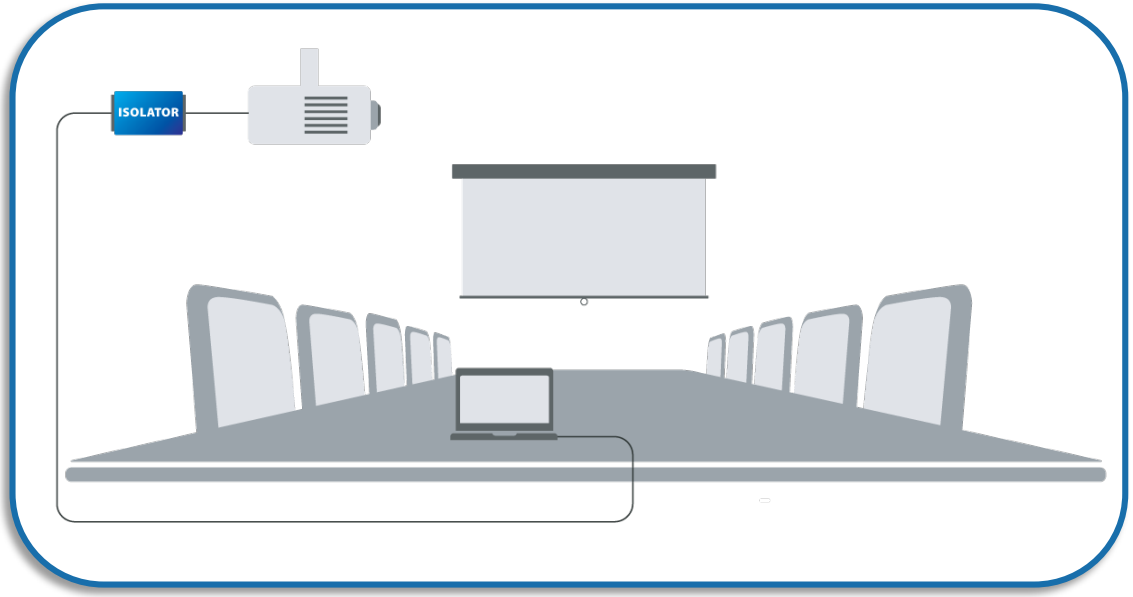


HighSecLabs
Highest Security Solutions Ltd.

Isolator Unidirectional Extenders

Secure DP/HDMI KVMA or Video only Isolators

- Designed to support isolation of large KVM matrix and conference room equipment (like projectors)
- Prevents host-to-peripheral direct access and eliminates data leakages by ensuring data flow in a single direction



Secure Unidirectional Copper or Fiber Extenders

- For connecting remotely to peripherals in other rooms of the building
- Copper or Optical Fiber data transmission for large distances

HighSecLabs
Highest Security Solutions Ltd.

Secure Supply Chain and Product Clearance

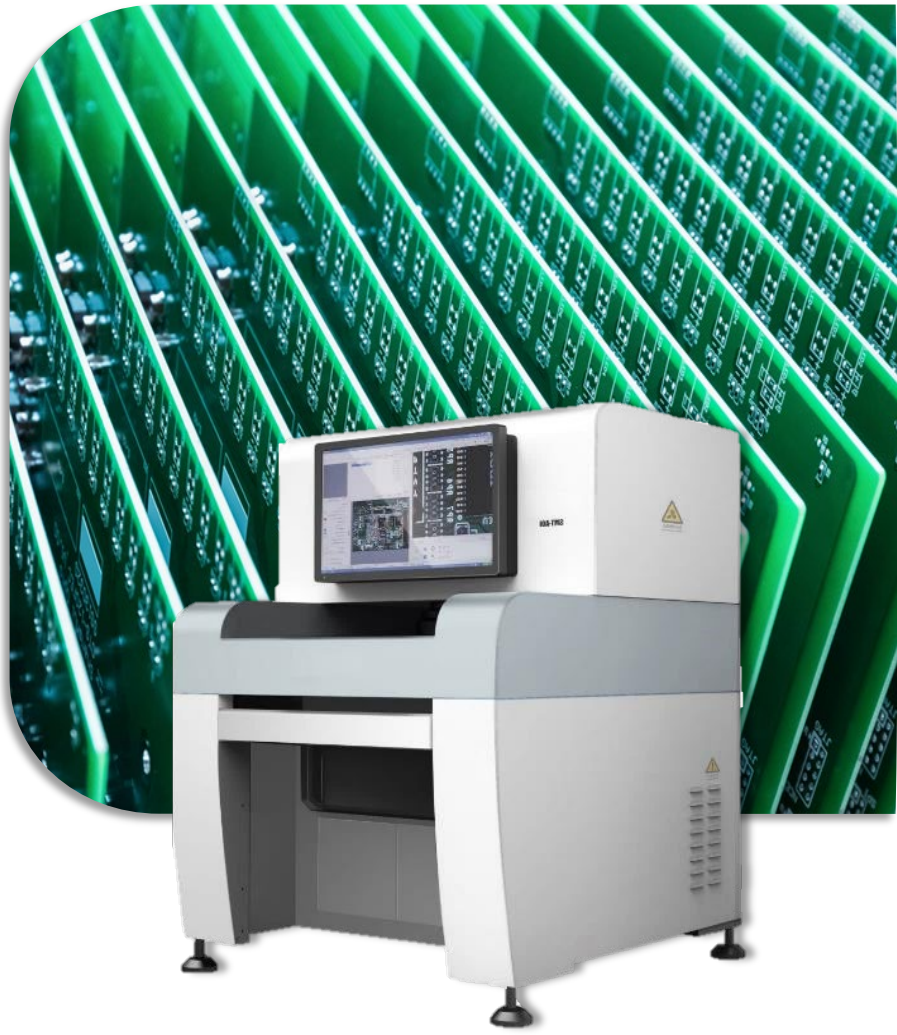
HSL Secure Desktop and Supply Chain Solutions

Users in sensitive and secure environments are facing additional cyber risks originating from different commercial devices used by them.

Despite network isolation, infiltrating a secure network is possible via supply chain attacks and the use of open interfaces on computers connected to secure or unsecure networks.

High Sec Labs (HSL's) approach is to attack the issue on both levels:

- Secure Supply Chain
- Protect open peripheral ports via a custom set of products

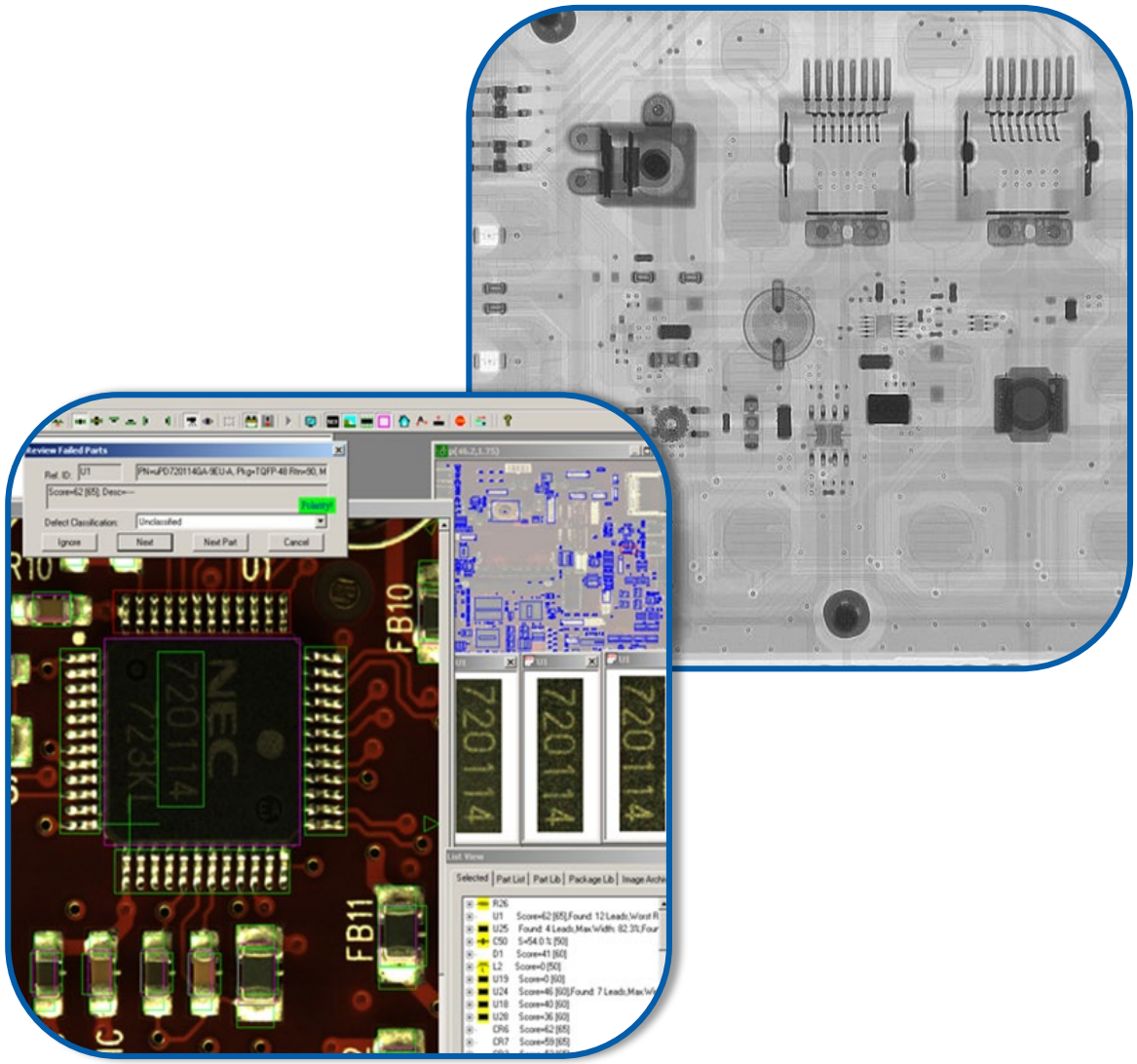


HighSecLabs Highest Security Solutions Ltd.

Secure Supply Chain Service

HSL's Secure supply chain service includes:

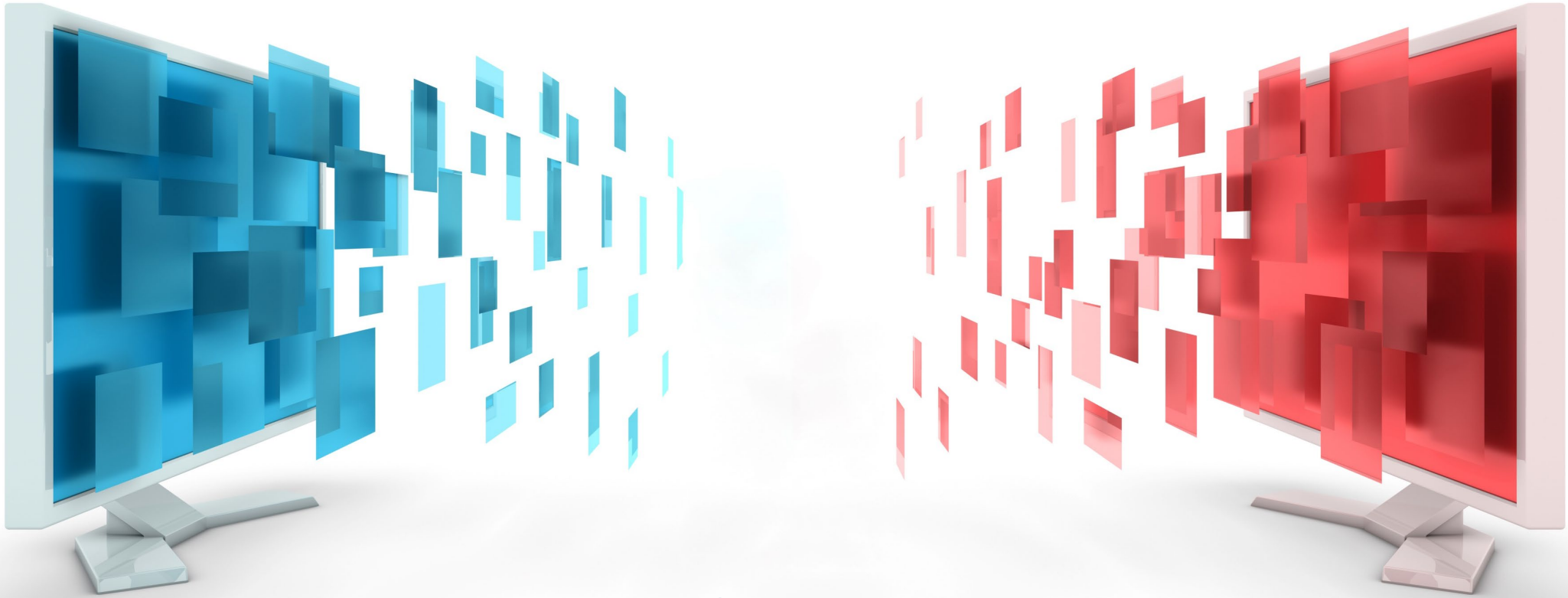
- Use of comparative X-ray to assure no unknown components on acquired products
- Utilize AOI machine for in depth board comparison
- Create a full engineering reverse design file to identify potential weakness
- Removing and blocking components and remove open functions
- Creating a test plan based on sampling to assure supply chain credibility



HighSecLabs
Highest Security Solutions Ltd.

THANK YOU

HighSecLabs
Highest Security Solutions Ltd.

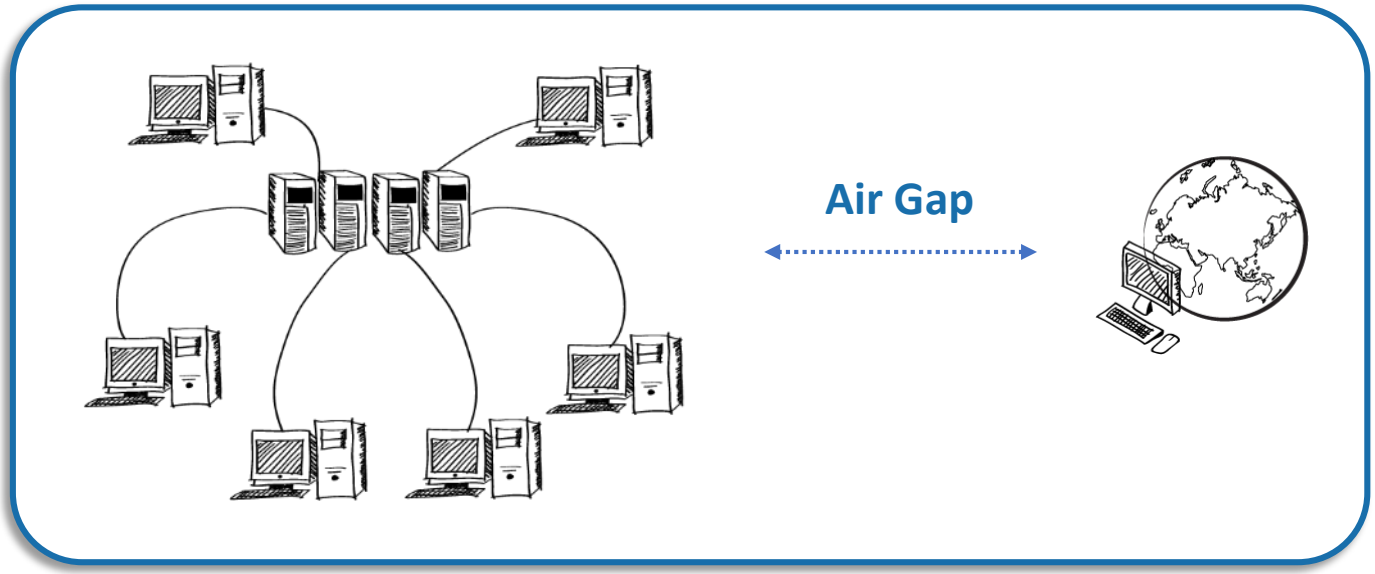


Field of Operation: what is airgap?

Air Gap

Definition

A cyber security measure that secures computer network by physically isolating it from unsecured networks, such as the Internet or another unsecured local area networks.



Examples of the types of networks or systems that may be air gapped:

- Military defence system
- Critical infrastructure command and control centres
- Computerized medical equipment and healthcare
- Banking and finance sectors
- Cryptocurrencies air-gapped (‘cold’) wallets, blockchain

Threats – Chain of Attack

Infiltration	How can attackers place a malware in the air gapped network?	
C&C	How can attackers send commands to the malware in the air-gapped network?	
Exfiltration	How can attacker leak data from the air gapped network?	

HighSecLabs
Highest Security Solutions Ltd.

Infiltration

Despite the level of isolation, air-gapped networks are not immune to breaches

- Supply Chain Attacks
- Malicious Insiders
- Deceived Insiders

Infiltration – Example 1

The Register®
Biting the hand that feeds IT

Jul 2018

Security

No big deal... Kremlin hackers 'jumped air-gapped networks' to pwn US power utilities

'Hundreds' of intrusions, switch could be pulled anytime, where have we heard this before?

By Richard Chirgwin 24 Jul 2018 at 05:28 80 SHARE ▼

The US Department of Homeland Security is once again accusing Russian government hackers of penetrating America's critical infrastructure.

Uncle Sam's finest reckon Moscow's agents managed to infiltrate computers networks within US electric utilities – to the point where the miscreants could have virtually pressed the off switch in control rooms, yanked the plug on the Yanks, and plunged America into darkness.

The hackers, dubbed Dragonfly and Energetic Bear, struck in the spring of 2016, and continued throughout 2017 and into 2018, even invading air-gapped networks, it is claimed.

HighSecLabs
Highest Security Solutions Ltd.

Infiltration – Example 2

- US military base in the Middle East
- A USB flash drive infected with a worm (Agent.BTZ) was left in the parking lot
- Inserted into a laptop that attached to the United States Central Command network
- From there it spread undetected to other classified and unclassified networks
- The Pentagon spent nearly a year cleaning the worm from military networks