ihse.

CERTIFIED SOLUTIONS

PROTECTED DATA TRANSMISSION IN HIGH-SECURITY ENVIRONMENTS

EAL+ CERTIFIED FOR MAXIMUM DATA SECURITY

WHEN UNCOMPROMISING SECURITY IS REQUIRED

The modern defense IT community is coming under ever increasing and sophisticated computing threats ranging from simple data theft from open USB ports to sophisticated hacking via malicious code or other determined insider activity.

Unisolated and 2-way communication via the USB, audio and video interfaces represents a specific hacking opportunity and a hidden risk to defense computer managers.

Examples include:

- an open USB interface being used to steal data or to inject malicious software
- the audio speaker channel being used in reverse as a microphone to eavesdrop on in-room audio
- high frequency (out-of-band) audio being used as a data-stream to send data undetected

IHSE's new range of isolated secure extenders prevent these types of threat by incorporating internal low-pass filters which block any out-of-range audio and a unidirectional data-diode that prevents the injection of malicious code via the upstream data path on USB-HID, video and audio channels.

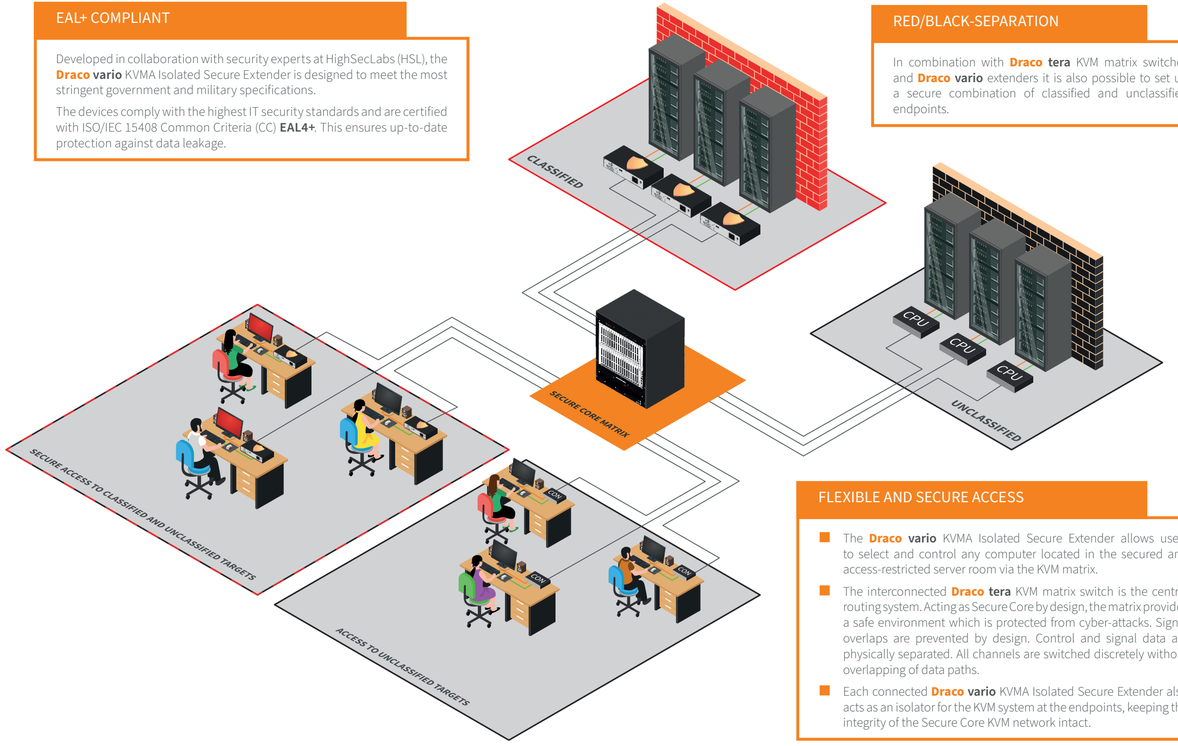
CYBER-RESILIENT COMPUTER ACCESS

The **Draco vario** KVMA Isolated Secure Extender provides an excellent security concept to maintain complete data integrity and prevent unauthorized access. **Draco tera** systems enable protected computer access and secure sharing and switching between computers. Users can safely and conveniently switch between resources operating at multiple classification levels.

EAL+ COMPLIANT

Developed in collaboration with security experts at HighSecLabs (HSL), the **Draco vario** KVMA Isolated Secure Extender is designed to meet the most stringent government and military specifications.

The devices comply with the highest IT security standards and are certified with ISO/IEC 15408 Common Criteria (CC) **EAL4+**. This ensures up-to-date protection against data leakage.



RED/BLACK-SEPARATION

In combination with **Draco tera** KVM matrix switches and **Draco vario** extenders it is also possible to set up a secure combination of classified and unclassified endpoints.

FLEXIBLE AND SECURE ACCESS

- The **Draco vario** KVMA Isolated Secure Extender allows users to select and control any computer located in the secured and access-restricted server room via the KVM matrix.
- The interconnected **Draco tera** KVM matrix switch is the central routing system. Acting as Secure Core by design, the matrix provides a safe environment which is protected from cyber-attacks. Signal overlaps are prevented by design. Control and signal data are physically separated. All channels are switched discretely without overlapping of data paths.
- Each connected **Draco vario** KVMA Isolated Secure Extender also acts as an isolator for the KVM system at the endpoints, keeping the integrity of the Secure Core KVM network intact.

FLEXIBLE COMBINATION WITH MAXIMUM PERFORMANCE

Draco vario KVMA Isolated Secure Extenders

Provides secure access and latency free operation of remote computers and systems. Keyboard, video, mouse and audio signals are transmitted via proprietary coding, all isolated and protected by intermediate advanced security layers. Suitable for point-to-point connections as well as complex KVM matrix switching networks.

- DisplayPort and HDMI combo jack
- Resolutions: 1920 x 1200 @ 60 Hz | Full HD | 2K HD
- 2-channel PCM embedded digital audio and analog audio
- Cat X and fiber versions; redundant data links available

Draco vario Extenders

Traditional **Draco vario** KVM extenders transmit computer signals via proprietary coding. They are designed for the use with **Draco tera** KVM matrix systems and are suitable for combined operation with **Draco vario** KVMA Isolated Secure Extenders. This allows switching between classified and unclassified sources clearly defined by assigned access rights.

SEPARATION OF RED AND BLACK ENVIRONMENTS

The IHSE KVM system enables precise access rights management, as required in government and military installations to separate classified and unclassified data and environments.

HIGH INVESTMENT SECURITY

The system supports most current display resolutions and is already prepared for many future formats. This means that the **Draco vario** KVMA Isolated Secure Extender represents a long-lasting, high-ROI investment that will scale with user demands for years to come.

Draco tera

TOTAL CONNECTIVITY AND FLEXIBLE SWITCHING

The **Draco tera** range extends from 8 to 576 non-blocking assignable ports. With mixed operation over copper and fiber cables, the switches handle all types of computer signals including USB, audio and video (HD, 4K, 8K above).

Draco tera is designed for 24/7 mission critical operation with extensive redundancy features and hot-swap option of components. Users can instantaneously access any computer-based control and information system at the best possible video quality. Due to integral switching and access management, the system can be operated completely independently of IP infrastructure. The strict separation of control and data signals and interference-free signal transmission provide additional protection for the system.

ihse.

IDENTIFY AND ELIMINATE DATA SECURITY THREATS

UNAUTHORIZED DATA ACCESS

Access control lists, managed on matrix configuration level, limit users and workstations to specific CPUs and levels. In addition, IHSE provides monitoring options in case of rights violations.

INFILTRATION OF MALWARE

HID allows the connection of keyboard and pointing devices only, providing hardware protection against unauthorized data injection.

DATA THEFT

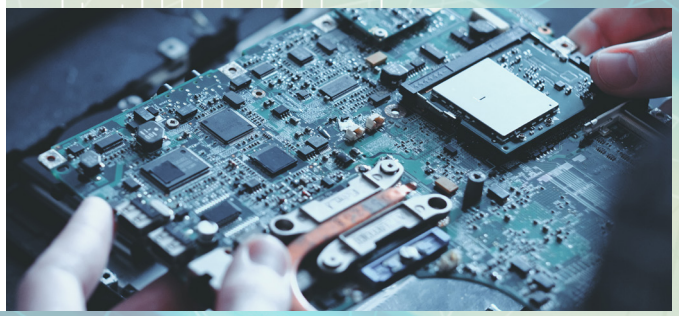
Restricted USB access prevents unauthorized mass data copy onto remote storage devices.

EAVESDROPPING

Attempts to intercept or access data carried on a KVM system are defended through the use of proprietary hardware devices. Audio signals can only be transmitted one-way from the source to the user, which prevents potential audio signal interception.

HIGH-FREQUENCY AUDIO

A low-pass filter prevents malicious use of out-of-band audio.



EXTERNAL CONTROL ATTEMPTS

Optional in-band control for safety-critical installations prevents switching via external media control. The core matrix is physically separated from the IP network, excluding potential hacker attacks via IP by design.

HEADQUARTERS

IHSE GmbH
Benzstr. 1
88094 Oberteuringen
Germany

Tel.: +49 (7546) 9248-0
info@ihse.com

SUBSIDIARIES

IHSE USA LLC
1 Corporate Drive
Cranbury, NJ 08512
USA

Tel.: +1 (732) 738 878 0
info-usa@ihse.com

IHSE GmbH Asia Pacific Pte Ltd
158 Kallang Way, #07-13A
Singapore 349245

Tel.: +65 (6841) 470 7
info-apac@ihse.com

REGIONAL REPRESENTATIVES

Shoham, Israel
Tel.: +972 (544) 320 768
info@ihse.com

Seoul, South Korea
Tel.: +82 (103) 752 401 3
info@ihse.com