

WHITE PAPER

SECURING
Multi-Domain KVM & Video with Neous

Centralized access control, hardware-enforced isolation, and AES-256-GCM encryption for real-time video and HID traffic

HighSecLabs
Highest Security Solutions

HLT39923 Rev 1.0

TABLE OF CONTACTS

Executive Summary 3

The Challenge 4

Typical Deployments 4

Neous Secure Architecture 5

- Centralized access control 6
- Hardware isolation at every boundary 6
- End-to-end encryption for video and HID 7

Why AES-256-GCM 8

Security Without Sacrificing Performance 8

Standards and Assurance 9

Scenario: The Insider on the Network 10

Conclusion 12

EXECUTIVE SUMMARY

Command and control centers, SOCs, and intelligence facilities need operators to see and control systems across classified, restricted, and unclassified networks from a single position—without compromising the isolation between those domains. At the same time, the video and keyboard/mouse traffic required for remote operation must traverse IP networks that cannot be assumed to be trusted in a high-assurance environment.

High Sec Labs (HSL) addresses these challenges with Neous, a secure KVM-over-IP platform built around a layered, Zero Trust security architecture.

- **Centralized authentication and authorization** — The Neous Management System authenticates endpoints, manages user and source permissions, controls connections, and distributes encryption keys only between approved endpoints.
- **Network access control** — 802.1X and endpoint authentication prevent unauthorized devices from gaining access to the Neous network and establishing connections.
- **Hardware-enforced isolation** — HSL Encrypted Isolators are deployed at the Transmitter and Receiver endpoints to enforce strict one-way data paths and allow only the video and HID traffic required for operation, preventing unauthorized data injection or unintended return paths to connected computers.
- **End-to-end encryption** — Phylax, HSL's encryption architecture based on AES-256-GCM, protects video and HID data in transit. Captured network traffic cannot be decrypted without the required encryption keys.
- **Hardware-based security controls** — Isolation and cryptographic protection are implemented using dedicated hardware and FIPS 140-3-compliant cryptography, providing strong security without compromising the low latency required for real-time operations.

Together, these controls provide defense in depth, preventing unauthorized access, enforcing one-way data flow, and protecting data in transit. Neous delivers secure, real-time access across isolated networks without compromising security or performance.

THE CHALLENGE

Multi-domain environments place three demands on a KVM and video infrastructure.

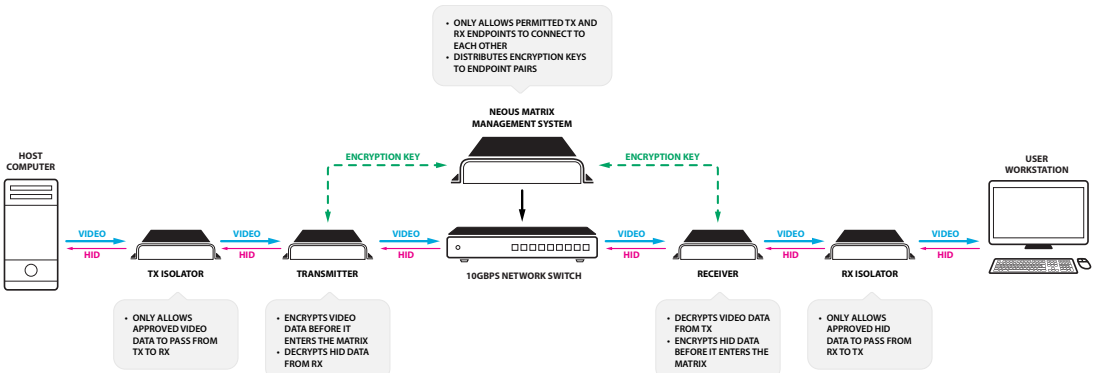
- **Strict separation:** Operators must work across networks of different classifications, but no data can be allowed to leak between them, whether by accident or through deliberate exploitation of side channels in video and USB interfaces.
- **Protection in transit:** Video streams can reveal application screens, credentials, and operational information. Keyboard and mouse traffic are small in volume but provides direct control of connected systems. Controlling access to the network is not enough; the data itself must be protected while it travels.
- **Real-time performance:** Video is a continuous, high-bandwidth stream, and HID input is highly time-sensitive. Any security measure that adds noticeable latency degrades the operator experience and risks compromising the mission.

TYPICAL DEPLOYMENTS

Neous is suited to any environment that requires secure access to multiple networks and systems, including:

- Military command and control centers
- Security Operations Centers (SOCs)
- Intelligence and classified environments
- Critical infrastructure and industrial control rooms
- Video walls and monitoring centers supporting multiple security classifications

NEOUS SECURE ARCHITECTURE



Neous employs multiple layers of security to protect connected devices, control access, enforce data-flow restrictions, and secure data in transit.

CENTRALIZED ACCESS CONTROL

The Neous Matrix Management System centrally manages connections between Transmitter (TX) and Receiver (RX) Endpoints.

- **Permission-based access**: Each Endpoint is assigned permissions that determine which connections are authorized.
- **Centralized control:** All Endpoint connections are established and overseen by the management system.
- **Controlled key distribution:** Encryption keys are distributed only between authorized Endpoints.

This ensures that users can access only sources permitted by their classification, reinforcing domain separation through centralized policy enforcement.

HARDWARE ISOLATION AT EVERY BOUNDARY

Every Neous TX and RX Endpoint is paired with a dedicated HSL Encrypted Isolator. Endpoints verify the Isolator's presence at startup and will not operate without it.

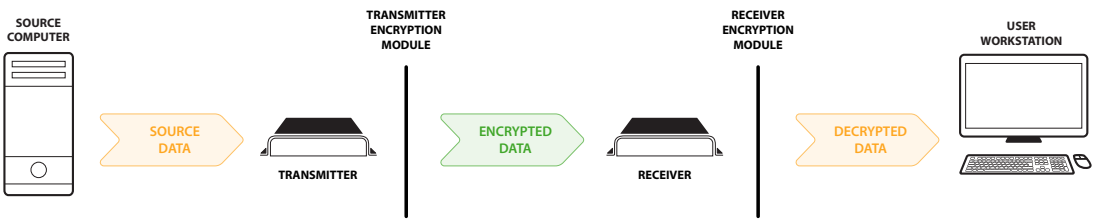
- **One-way video:** Video flows from source computers to user displays.
- **One-way HID:** Validated keyboard and mouse traffic flows from user workstations to source computers.

Encrypted Isolators can also secure existing KVM and video-switching infrastructure, strengthening protection without requiring replacement of established systems.

END-TO-END ENCRYPTION FOR VIDEO AND HID

While centralized access control governs connections and hardware isolation restricts data flow, HSL's Phylax encryption architecture protects data in transit between authorized Endpoints.

Each TX and RX Endpoint contains a Phylax encryption module that encrypts data before network transmission and decrypts it only at the authorized destination.



Independent encryption engines protect both channels:

- **Video:** Real-time encryption and authentication protect video streams in transit while supporting responsive, high-resolution operation.
- **HID:** Keyboard and mouse reports undergo HSL's HID filtering before encryption and authentication. At the receiving Endpoint, the reports are decrypted and verified before reaching the destination computer, preserving normal HID functionality.

WHY AES-256-GCM

Phylax uses AES-256 in Galois/Counter Mode (GCM), an internationally recognized standard for authenticated encryption. While Phylax is proprietary, its cryptographic foundation relies on a proven, standardized algorithm.

AES-256-GCM provides two essential security properties:

- **Confidentiality:** Captured network traffic cannot be decrypted without the required key.
- **Authentication and integrity:** Receivers verify data authenticity and integrity, detecting and discarding modified or unauthenticated packets.

For KVM systems, both are critical: confidentiality protects what operators see, while integrity protects the commands they issue.

The Neous Matrix Management System coordinates key distribution using ECDH-based authenticated key exchange. Support for externally provisioned keys and secure in-band key exchange allows organizations to align key management with their security policies.

SECURITY WITHOUT SACRIFICING PERFORMANCE

Neous performs cryptographic processing in dedicated hardware integrated directly into the data path, delivering the throughput required for continuous high-resolution video and the low latency essential for responsive keyboard and mouse control.

HSL's implementation combines the benefits of standardized cryptography with purpose-built hardware. While the underlying architecture and optimization techniques remain proprietary, customers benefit from secure, real-time operation without needing access to HSL's internal design.

STANDARDS AND ASSURANCE

For government, defense, and other security-sensitive environments, security depends on both the cryptographic algorithms and how they are implemented. Neous incorporates recognized standards and hardware-based security controls, including:

- **NIAP-certified isolation:** Hardware-enforced isolation using HSL's certified security technologies.
- **FIPS 140-3-compliant cryptography:** AES-256-GCM encryption within the Phylax architecture.
- **Hardware root of trust:** Secure boot, TrustZone, and tamper protections to safeguard Endpoint integrity and cryptographic functions.
- **Trusted random number generation:** Hardware-based random number generation designed to meet applicable NIST requirements.
- **802.1X network access control:** Authentication to restrict network access to authorized devices.

SCENARIO:
THE INSIDER ON THE NETWORK

Consider a rogue network administrator or compromised insider with full access to the IP switching infrastructure, but no access to the cryptographic keys held by authorized Neous Endpoints. The attacker captures traffic between an operator's Receiver (RX) and a remote server's Transmitter (TX), aiming to recover keystrokes, replay input, or inject malicious commands.

- **Attempting to intercept data:** Captured traffic is encrypted using AES-256-GCM. Without the required keys, the attacker cannot recover the underlying keyboard, mouse, or video data.
- **Attempting to inject commands:** Commands injected without the correct encryption key cannot be correctly decrypted by the Encrypted Isolator. The resulting data is unintelligible to the connected computer, preventing the injected commands from being executed as intended.
- **Attempting to gain unauthorized access:** Network access controls restrict unauthorized devices, while the Neous Matrix Management System controls Endpoint authorization and key distribution. If the system identifies unauthorized devices or suspicious activity, it can remove them from the network.
- **Attempting to bypass hardware isolation:** Neous Endpoints verify the presence of their required Encrypted Isolators and will not function without them. Disconnecting an Isolator therefore disables the associated Endpoint rather than providing a path around the security controls.

Together, these mechanisms protect data confidentiality, prevent unauthorized input from being interpreted as valid commands, restrict unauthorized network access, and preserve hardware-enforced isolation.

Each attempted attack fails because the Neous secure architecture closes a different avenue:

Security Layer	Protection Provided
Neous Matrix Management System	Enforces permission-based connections between authorized Endpoints and controls encryption-key distribution.
NIAP-certified Encrypted Isolator	Enforces hardware-based data-flow restrictions, allowing approved video and HID traffic while blocking unauthorized channels and signal paths.
Phylax AES-256-GCM encryption	Protects video and HID confidentiality, preventing disclosure of content to parties without the required keys.
Authenticated integrity protection	Verifies packet authenticity and integrity, allowing modified or unauthenticated packets to be rejected.
Authenticated ECDH-based key exchange	Establishes shared session keys between authorized Endpoints while protecting key establishment against unauthorized parties, subject to the authentication protocol.
Secure boot and TrustZone	Help protect endpoint integrity and isolate sensitive cryptographic operations.
802.1X and Network Access Control (NAC)	Restrict network access to authenticated and authorized devices.

CONCLUSION

Neous enables secure, multi-domain operations over shared KVM and video infrastructure without compromising domain separation. Centralized access control governs authorized connections, HSL Encrypted Isolators enforce hardware-based data-flow restrictions, and Phylax encryption protects video and HID data in transit using AES-256-GCM.

Together, these controls provide defense in depth across access, isolation, and data protection—delivering secure, responsive operation over multi-domain IP networks.

> Only authorized Endpoints can establish approved connections. Data remains encrypted in transit, while hardware isolation restricts traffic to its intended direction and purpose—all without sacrificing real-time performance.

www.highseclabs.com

High Sec Labs (HSL) develops high-quality cyber-defense solutions in the field of network and peripheral isolation for protecting national assets and infrastructure.

The company, headquartered in Or Akiva, Israel, was founded in 2008 and has a second manufacturing site in the United States.

High Sec Lab's roots are deeply embedded in the defense and commercial industries developing cyber protection solutions. Among its customers are some of the world's leading governments and defense organizations as well as commercial companies such as banks, healthcare providers, and national infrastructure companies.

HighSecLabs
Highest Security Solutions

© 2026 HighSecLabs Ltd. All rights reserved. All trade names are trademarks or registered trademarks of respective manufacturers listed.
Specifications are subjected to change without prior notice. Patents: www.highseclabs.com/patents/. HLT39923 Rev 1.0