seclab®

Resilience and Control through Network Isolation

WHITE PAPER

seclab-security.com

Table of contents

Introduction

In today's hyper-connected digital landscape, organizations face unprecedented cyber-security challenges. As systems become increasingly interconnected, the attack surface expands exponentially, creating new vulnerabilities that sophisticated threat actors are quick to exploit.

8.4 trillon $

The global cost of cybercrime reached approximately $8.4 trillion in 2023 – a figure that encompasses direct losses, remediation costs, business disruption, and reputational damage.

Source : Cybersecurity Ventures

This growing threat landscape, accelerated by advancements in artificial intelligence and the professionalization of cyber criminals, demands robust protection strategies for critical infrastructure and sensitive systems. While traditional security approaches like firewalls have long been standard defensive measures, they increasingly fall short against advanced persistent threats and sophisticated attack methodologies.

Network isolation has emerged as a critical security paradigm for protecting sensitive systems from external threats. But what exactly constitutes effective isolation in cyber-security? How does it differ from mere segmentation? And how can organizations achieve true network isolation without sacrificing the operational functionality required in today's interconnected environments?

This white paper explores these questions and introduces SECLAB's revolutionary Electronic Isolation technology: a breakthrough approach that delivers comprehensive network isolation while enabling the bidirectional communication essential for modern operations.

Network Segregation: A True Need

Understanding Network Segregation

Network segregation represents a fundamental security strategy that physically separates different network environments to prevent lateral movement of threats and unauthorized access between systems. Unlike segmentation, which merely divides networks logically through virtual controls, true segregation creates distinct network zones with controlled, monitored interfaces between them.

Network segregation creates separate zones within a network where data and user activity are confined. If one segment becomes compromised, the segregation prevents threat propagation, significantly limiting the impact of security incidents. When implemented correctly, network segregation provides:

- Prevention of lateral movement during attacks
- Containment of compromised systems
- Protection of sensitive data from unauthorized access
- Reduced attack surface for critical systems
- Enhanced compliance with regulatory requirements

Regulatory Requirements for Network Segregation

Network segregation has become a cornerstone requirement across numerous international cybersecurity regulations and frameworks, including:

- **IEC 62443:** International industrial automation and control systems security standards that mandate network segmentation and segregation.
- **NERC CIP Standards:** Mandatory reliability standards for North American power grid operators that specify network isolation requirements.
- **NIS/NIS2 Directives:** European regulations requiring critical infrastructure providers to implement appropriate security measures, including network segregation.
- **DORA (Digital Operational Resilience Act):** European regulations requiring financial entities to implement robust ICT risk management.

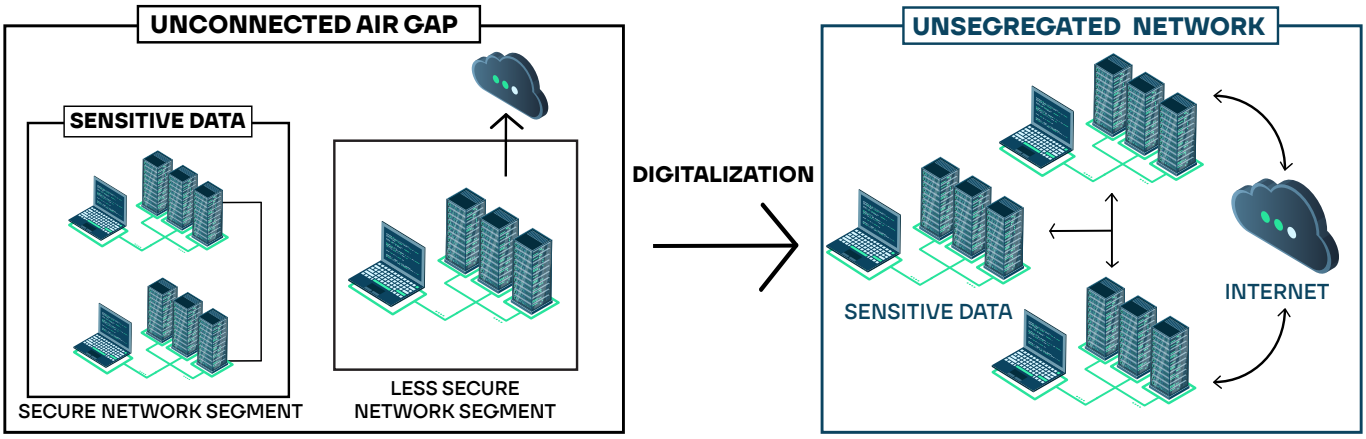
The Limitations of Physical Air Gaps

Traditionally, the most secure environments employed physical air gaps: completely disconnected networks with no digital communication pathways between systems.

While highly secure, this approach creates significant operational challenges:

- Impossible real-time data sharing between environments
- Inefficient manual data transfer processes
- Increased operational costs and personnel requirements
- Inhibited digital transformation and modernization efforts
- Potential for human error during manual transfers

As digital transformation accelerates across industries, the strict physical air gap approach has become increasingly impractical, driving the need for solutions that provide comparable security with greater operational flexibility.



Unsegregated network following digitalization

Firewalls Don't Isolate, They Filter

The Filtering Nature of Firewalls

Firewalls represent the most common network security technology, but it's crucial to understand their fundamental limitations. At their core, firewalls are sophisticated routing devices that filter traffic based on predefined rule sets.

When a packet meets the criteria defined in a firewall rule, it passes through unchanged to its destination. This fundamental design characteristic means firewalls:

- Allow direct network connections between separated environments
- Maintain the original network packet structure across boundaries
- Create bidirectional communication channels that can be exploited
- Expose the complete protocol stack to potential attacks

Inherent Vulnerability of the Firewall Model

The firewall security model contains several inherent weaknesses:

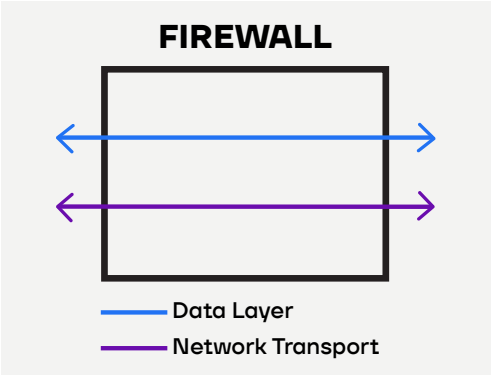
1. **Software-Based Protection:** Firewalls rely on software configurations that are susceptible to vulnerabilities, misconfigurations, and zero-day attacks
2. **Required Patching and Updates:** To maintain security, firewalls demand constant updates, creating potential windows of vulnerability
3. **Rule Complexity:** As rule sets grow increasingly complex, the potential for misconfiguration rises dramatically
4. **Exposed Protocol Stack:** By transmitting complete packets, firewalls expose network stacks, drivers, and OS components to attack
5. **Reconnaissance Enablement:** Firewalls often allow network scanning traffic, enabling attackers to map protected networks

Firewalls: Designed for Segmentation, Not Segregation

It's critical to understand that firewalls were never designed for true network segregation. Their core functionality centers on controlled interconnection through packet filtering – essentially creating a permeable barrier rather than a true boundary.

This fundamental distinction explains why firewalls can be bypassed through:

- Advanced persistent threats that operate within allowed protocols
- Zero-day vulnerabilities in firewall software
- Complex rule sets that inadvertently create security gaps
- Social engineering tactics that compromise credentials
- Malicious insider threats leveraging legitimate access



Firewall Operation

Data Diodes: Outdated and Impractical

The Origins and Mechanics of Data Diodes

Data diodes emerged from military and intelligence needs for physically enforced one-way information flow. The technology relies on a simple principle: data can enter but never leave a protected environment. At their core, data diodes employ:

- An optical fiber with a transmitter on one side and a receiver on the other
- Hardware that physically enforces unidirectional data flow
- No software components that could be compromised

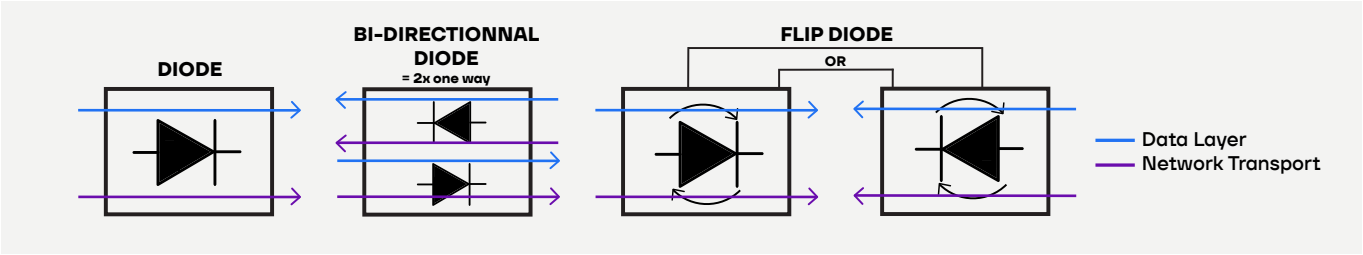
This hardware-enforced approach offers exceptional security for specific use cases but comes with significant functional limitations.

The Unidirectional Reality of Data Diodes

Despite marketing claims about « bidirectional data diodes, » these solutions invariably fall into one of three categories:

1. **Paired unidirectional diodes:** Two separate data diodes allowing independent one-way traffic in opposite directions
2. **Reversible diodes:** Systems that can operate in either direction, but never simultaneously
3. **Hybrid architectures:** Combinations of diodes with timed, air-gapped firewalls

These approaches attempt to address the fundamental problem with data diodes: their inherent inability to support bidirectional protocols like TCP/IP that require acknowledgment packets.



Different Types of Diode Operation

Protocol Compatibility Challenges

Data diodes face significant challenges with modern network protocols:

UDP Implementation:

- Requires « gates » (computers) on both sides of the diode
- Enables IP addressing but still loses UDP response packets
- Functions adequately for stateless communications only

TCP/IP Handling:

- Requires protocol-aware proxies on both sides
- Input gate must simulate responses to clients
- Output gate can only initiate new connections to servers
- Server responses received by output gate must be discarded
- Limited to specifically supported protocols

For encrypted communications, data diodes face even greater challenges, as they disrupt the bidirectional key exchange required by modern encryption protocols. This forces organizations to either:

- Manually exchange encryption keys (undermining security)
- Use the data diode itself as a cryptographic endpoint (creating a new attack surface)
- Implement complex workarounds with limited protocol support

SECLAB Electronic Isolation: A Paradigm Shift

A Technology Born from Operational Necessity

SECLAB's Electronic Isolation technology emerged from a critical need expressed by industrial customers: How to achieve the security of physical network isolation while maintaining the operational functionality of bidirectional communications.

Developed and refined over a decade of deployments in the most demanding environments, including military installations, nuclear facilities, railway control systems, and hydroelectric infrastructure, this patented technology represents a fundamental breakthrough in network security.

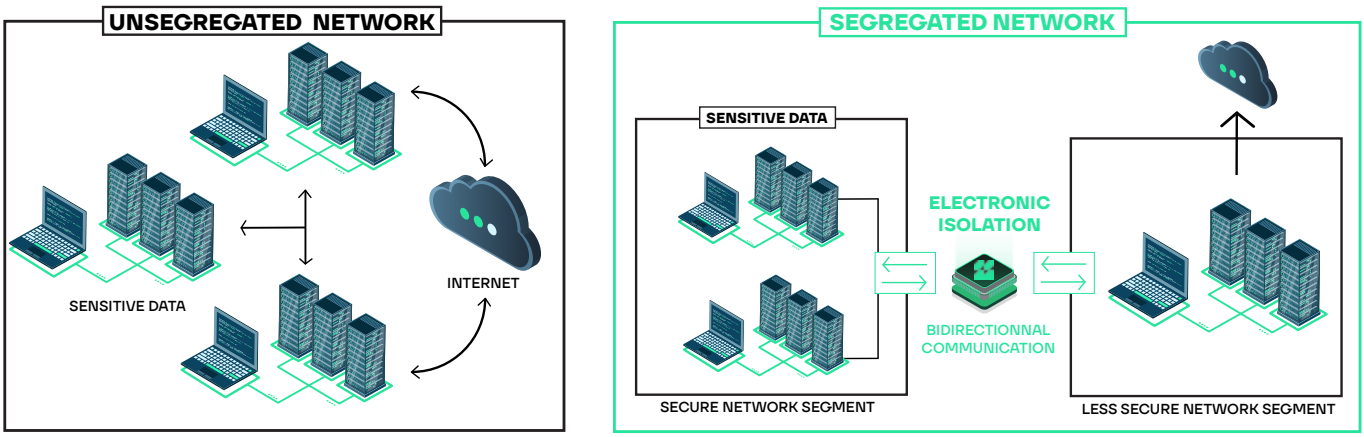
Seclab Secure Xchange Network

The Electronic Isolation Advantage

SECLAB's Electronic Isolation technology, embedded in the SecXN product line, delivers true network segregation through a revolutionary approach:

1. **Complete Protocol Breaking**: Rather than simply filtering packets, SecXN completely strips away and reconstructs network protocols (OSI layers 1-4).
2. **Payload Preservation:** While network layers are destroyed and rebuilt, the application data (layers 5-7) remains intact, enabling full functionality.
3. **Hardware-Enforced Security:** This process occurs at the hardware level through specialized electronic circuits rather than vulnerable software components.

This approach effectively creates an « electronic air gap » between networks while still enabling controlled data exchange – delivering security comparable to physical isolation with the operational benefits of interconnection.



Segregated Network with Bidirectionnal Communication through Electronic Isolation compared to an Unsegregated Network

How Electronic Isolation Technology Works

The SecXN implements Electronic Isolation technology through a three-stage process:

Phase 1 : Stripping	Phase 2 : Transmission	Phase 3 : Reconstruction
Each IP packet from the source network has layers 1-4 completely removed, leaving only the application payload (layers 5-7).	The payload passes through a dedicated hardware channel to the output side, with no transport information.	New, clean network layers 1-4 are generated and combined with the original payload before transmission to the destination network.

This patented process ensures that:

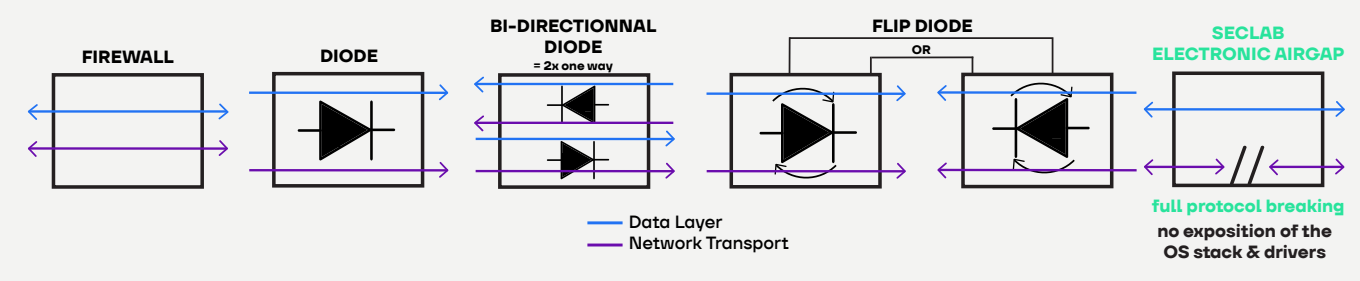
- No original network packets ever cross the boundary
- Transport-layer attacks cannot penetrate the protected network
- Network reconnaissance becomes impossible
- OS IP stacks, drivers, and network firmware remain protected
- Applications function normally without modification

Bidirectional Communications with Total Isolation

Unlike data diodes, SECLAB's Electronic Isolation technology supports true bidirectional communications without compromising security:

- **Full TCP/IP Support:** Enables bidirectional TCP/IP communications without protocol-specific customization
- **Encrypted Protocol Compatibility:** Works seamlessly with VPN, SSH, HTTPS, and other encrypted protocols
- **Native Application Support:** Requires no application modifications or special proxies
- **Direction Control:** Allows administrators to control which side can initiate specific types of connections

This unique capability addresses the fundamental limitation of data diodes while maintaining security superior to firewalls.



Firewall, Diodes and Seclab Electronic Isolation Operation Comparison

Comparative Analysis: Firewalls, Data Diodes, and Electronic Isolation

Customer Needs Analysis

Modern organizations express three critical security requirements that highlight the limitations of traditional approaches:

Need guarantee that no network traffic will ever enter OT network

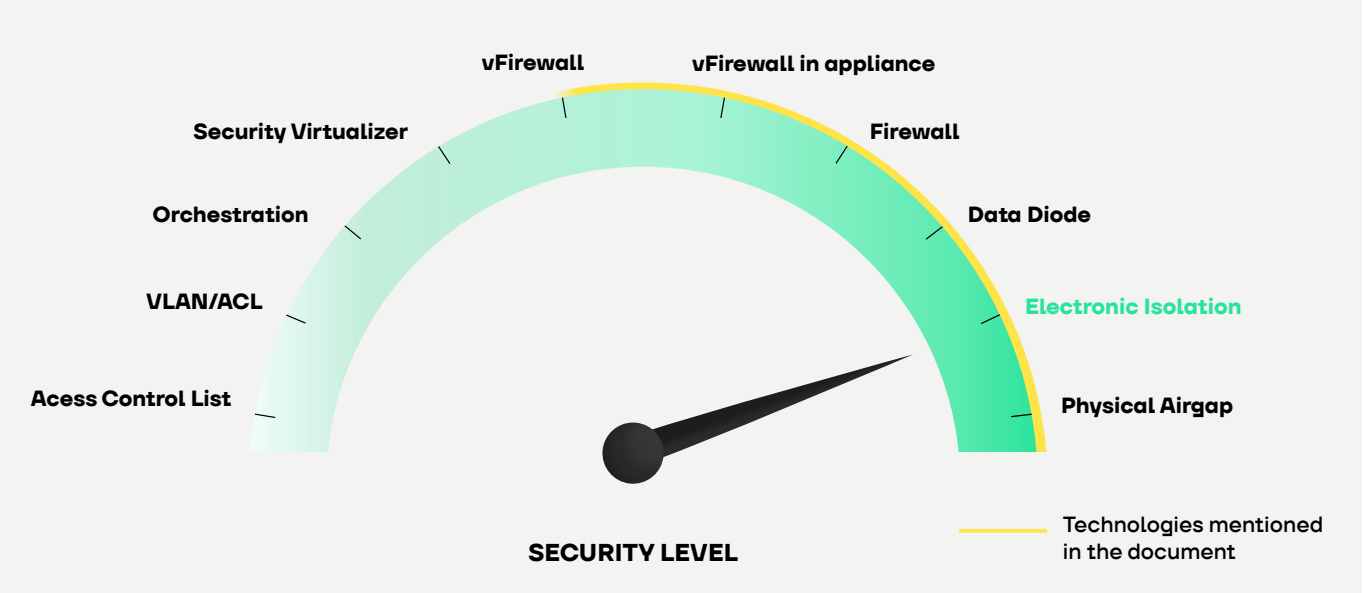
- Firewalls: Cannot provide this guarantee due to their filtering-based architecture
- Data Diodes: Meet this requirement but prevent essential bidirectional communications
- Electronic Isolation: Provide this guarantee while enabling full bidirectional functionality

Need to control networks interconnections

- Firewalls: Bring complexity in deployment and maintenance, are subject to vulnerabilities
- Data Diodes: Provide limited control in one direction only
- Electronic Isolation: Enable full control with dual administration (one per zone)

Need to use regular TCP/IP services between two networks that should not be connected to each other

- Firewalls: Are a cybersecurity SPOF (single point of failure)
- Data Diodes: Need gates to operate with TCP/IP, put constraints on used protocols, deny any acknowledgement
- Electronic Isolation: Full compliance with TCP/IP and UDP/IP-based protocols, never fails - no vulnerability can break the segregation



Security Level Gauge : Technologies comparison

The following three tables provide a comparative analysis across Security Architecture, Operational Capabilities, and Threat Protection for Firewalls, Data Diodes and Seclab Electronic Isolation.

Security Architecture Comparison

Feature	Firewalls	Data Diodes	SECLAB Electronic Isolation
Security Model	Software-based filtering	Hardware-enforced unidirectional flow	Hardware-enforced protocol breaking
Protocol Support	Full bidirectional ✓	Limited unidirectional	Full bidirectional ✓
Network Exposure	Direct network connectivity	No return path	Complete network isolation ✓
Vulnerability to Software Exploits	High	Low ✓	Low ✓
Need for Patching	Continuous	Minimal ✓	Minimal ✓
Reconnaissance Protection	Limited	Complete ✓	Complete ✓
Support for Standard Applications	Full ✓	Limited	Full ✓

Operational Capabilities Comparison

Capability	Firewalls	Data Diodes	SECLAB Electronic Isolation
Bidirectional Communicatinon	Yes ✓	No (with workarounds)	Yes ✓
TCP/IP Support	Full ✓	Limited/Proxied	Full ✓
Encrypted Protocol Support	Full ✓	Limited/Complex	Full ✓
Remote Management	Yes ✓	Limited	Yes (secured) ✓
Application Compatibility	High ✓	Low	High ✓
Implementation Complexity	Moderate	High	Easy to Moderate Limitation : can't be virtualised
Maintenance Requirements	High	Low ✓	Very Low ✓

Threat Protection Comparison			
Threat	**Firewalls Protection**	**Data Diodes Protection**	**SECLAB Electronic Isolation Protection**
Zero-day Exploits	Vulnerable	Only one direction Protected	Protected (both directions) ✓
Network Reconnaissance	Limited Protection	Strong Protection ✓	Strong Protection ✓
Lateral Movement	Limited Protection	Strong Protection ✓	Strong Protection ✓
Malformed Packets	Vulnerable	Protected (one direction)	Protected (both directions) ✓
Malicious Insider	Vulnerable	Limited Protection	Strong Protection ✓

Real-World Applications and Use Cases

Critical Infrastructure Protection

Electronic Isolation technology provides ideal protection for critical infrastructure environments where both security and operational functionality are essential:

- **Energy Production Facilities:** Protecting industrial control systems while enabling monitoring
- **Transportation Systems:** Securing railway signaling while maintaining operational visibility
- **Utilities Management:** Isolating SCADA systems while allowing data collection
- **Defense Installations:** Enabling controlled information sharing between security domains

Secure Remote Access and Monitoring

The bidirectional capabilities of Electronic Isolation technology make it particularly valuable for secure remote access scenarios:

- **Industrial Remote Maintenance:** Enabling vendor access without exposing critical systems
- **Secure Monitoring Solutions:** Allowing operational data collection without creating attack vectors
- **Emergency Response Systems:** Supporting critical communications during security incidents
- **IoT Security:** Creating secure zones for connected devices while maintaining control

Cyber Recovery and Business Continuity

Electronic Isolation technology provides the foundation for robust cyber recovery architectures that can withstand sophisticated attacks:

- **Isolated Backup Environments:** Enabling the creation of completely isolated backup environments that maintain operational connectivity
- **Clean Room Operations:** In the event of a significant cyber incident, enabling the establishment of clean room environments
- **Business Continuity Assurance:** Ensuring that cyber recovery doesn't require complete operational shutdown
- **Data Classification and Protection:** Enabling sophisticated data protection strategies

Regulatory Compliance

The SecXN helps organizations meet strict regulatory requirements for network segregation:

- **NERC CIP Compliance:** Meeting energy sector requirements for Electronic Security Perimeters
- **Defense Sector Standards:** Meeting stringent military-grade security requirements
- **NIS2 Directive Compliance:** Satisfying EU requirements for critical infrastructure protection
- **Financial Services Regulations:** Supporting DORA and other financial sector requirements

An appendix table presents a detailed breakdown of the latest standards and directives, highlighting their impact on organizations in terms of data protection.

Deployment Considerations

Integration with Existing Security Infrastructure

The SecXN is designed to complement and enhance existing security architectures:

- ✓ Operates transparently to applications and users
- ✓ Can be deployed alongside existing security tools
- ✓ Supports standard networking protocols and interfaces
- ✓ Requires minimal changes to existing network configurations

Deployment Models

Common deployment models for the SecXN include:

Gateway Deployment	Defense-in-Depth Deployment	Critical System Protection
• Positioned between network zones of different sensitivity • Controls all traffic between segregated environments • Provides centralized security enforcement	• Multiple SecXN devices creating security layers • Each layer implementing specific security policies • Progressive security enforcement throughout the network	• Dedicated SecXN devices protecting individual critical systems • Granular policy enforcement for specific applications • Maximum security for high-value assets

Administrative Considerations

The SecXN supports robust administrative controls:

- ✓ Separation of duties between security domains
- ✓ Multiple admins and roles with local password based authentication (don't rely on directories integrity)
- ✓ Comprehensive audit logging and monitoring
- ✓ Secure update mechanisms with cryptographic verification

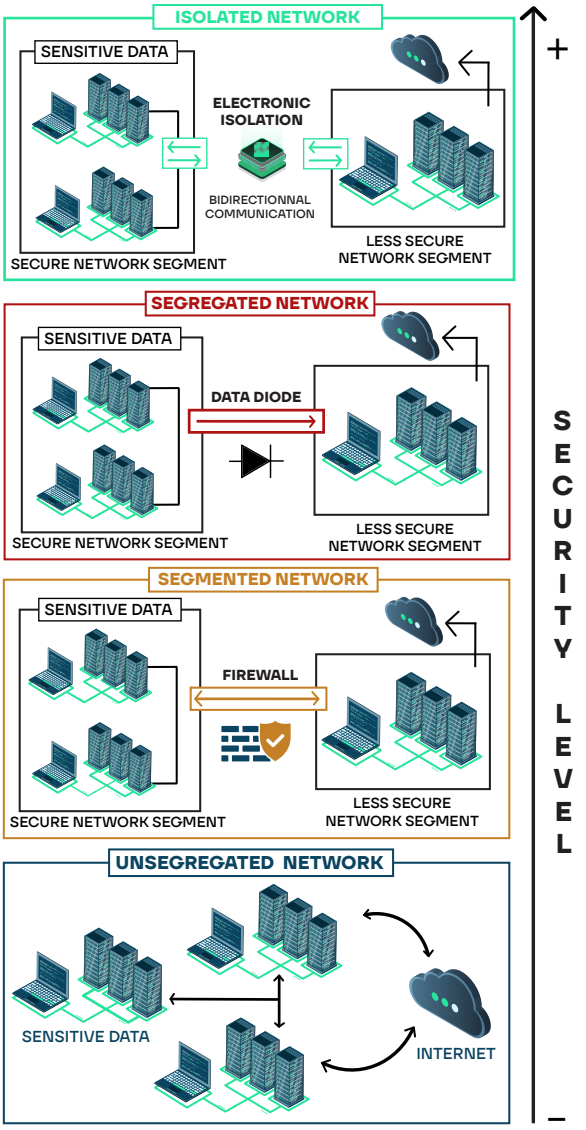
Conclusion

As cyber threats continue to evolve in sophistication and impact, organizations must adopt security approaches that provide true protection without compromising operational capability. Traditional technologies like firewalls and data diodes each present significant limitations in this regard: firewalls lack true isolation, while data diodes prevent essential bidirectional communications.

SECLAB's Electronic Isolation technology, embedded in the certified SecXN product line, represents a revolutionary approach to network segregation that addresses these limitations.

By combining hardware-enforced security with full protocol support, the technology delivers:

- ✓ True network isolation that prevents reconnaissance and lateral movement.
- ✓ Complete protection against transport-layer attacks in both directions.
- ✓ Full support for bidirectional communications including encrypted protocols.
- ✓ Transparent operation that requires no application modifications.
- ✓ Certified security validated by ANSSI (Secure Xchange Network (Sec-XN)Version 3.4.0 | ANSSI) and deployed in the most critical environments.



Comparison of Network Architectures Security Level

For organizations seeking to protect critical infrastructure, sensitive data, or regulated environments, SECLAB's Electronic Isolation technology offers an unmatched combination of security and functionality: true resilience and control through network isolation.

SECLAB Electronic Isolation: An easy way to use network services without network communications.

seclab.

Appendix

The latest standards and directives: what impact will data protection have on organizations?

Standards	Geographic areas concerned	Organisations targeted	Obligations	Recommendations
IEC 62443 Objective: To ensure the availability, integrity and confidentiality of IACS systems in industrial environments.	International	IEC 62443 is specifically designed for industrial automation and control systems (IACS).	IEC 62443 defines 7 essential security requirements, including user identification and authentication, privilege control, data integrity assurance, and resilience to attack.	IEC 62443 recommends the physical separation of critical and non-critical networks as a key measure for limiting the attack surface.
LPM Objective: To upgrade equipment, strengthen military intelligence and invest in cyber, solar, space and maritime defences.	International	The LPM is aimed at Operators of Vital Importance (OIV) and Vital Importance Information Systems (SIIV).	Rule 16 of the LPM requires partitioning measures to be taken.	These partitioning measures can be implemented through segmentation or physical isolation.
NIST Cybersecurity Framework (CSF) Objective: To help companies prioritise their areas for improvement and measure their progress in terms of cyber security.	International	The NIST Cybersecurity Framework is designed for different types of public and private organizations, from small businesses to large multinationals.	The NIST Cybersecurity Framework provides a framework for identifying risks, protecting information systems, detecting and managing cybersecurity vulnerabilities and recovering from them.	This process helps to raise awareness of shortcomings in terms of cyber risk management and to identify the protective measures that need to be implemented.
NERC-CIP Objective: To improve the security of electricity distribution systems by ensuring that appropriate measures are in place to protect against cyber-attacks and other security threats.	United States	NERC-CIP is aimed at electricity companies responsible for generating and managing electricity networks.	CIP-005 requires the creation of electronic security perimeters (ESPs) to separate cyber BES systems. CIP-015 calls for monitoring of traffic within ESPs.	NERC-CIP recommends the implementation of essential network segmentation to partition critical systems, defend against attacks, and limit exposure to external networks.
NIS 2 Objective: To strengthen the cyber security of the economic and administrative fabric of EU member states.	European Union	NIS2 is aimed at companies with more than 50 employees and certain local authorities with a turnover of more than €1m.	NIS 2 requires the protection of networks and information systems used to provide essential services in key sectors of our societies.	Legal, technical and organizational measures to be implemented, depending on the existing risk.
DORA Objective: Strengthen the cybersecurity and digital operational resilience of the financial sector.	European Union	DORA applies to the majority of financial entities.	DORA implicitly requires network segregation to limit the propagation of attacks, particularly for connected financial processes.	DORA encourages approaches such as micro-segmentation and Zero Trust.

seclab®

The Cyber-Physical systems company.

Contact us

contact@seclab-security.com

seclab-security.com

@Seclab

Montpellier Office
40 av. Théroigne de Méricourt,
34000 Montpellier, France

Paris Office
Landscape 22 Route de la Demi-Lune,
92800 Puteaux, France