seclāb

NEW LIFE FOR OLD SYSTEMS

WHITE PAPER • 2021

New life for old systems

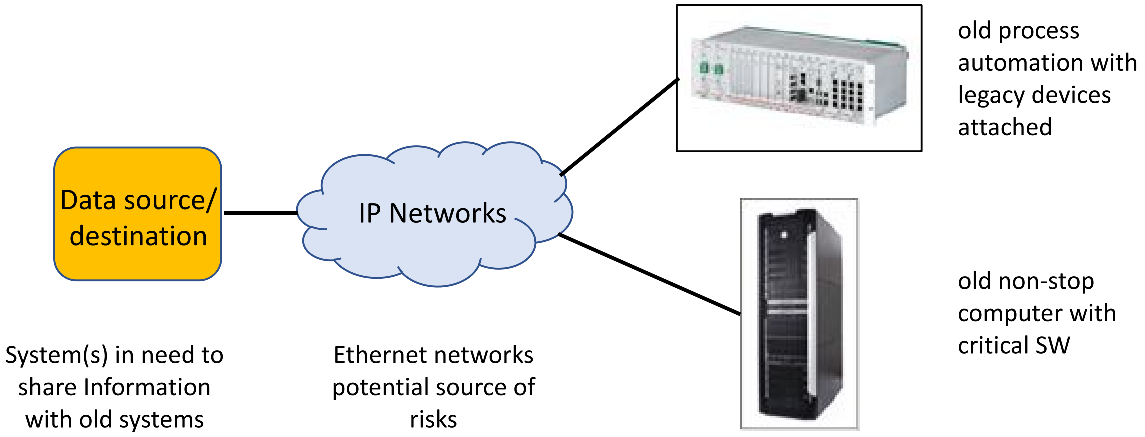
Included in a recent report (*), **Gartner** estimates that **in 2020**, **over 30% of successful attacks** suffered by enterprises will be on data located in **shadow IT resources**, such as abandoned, forgotten and legacy applications.

In numerous industries, **legacy systems** may be running on old hardware and/or using operating systems that **can't be easily updated but may be required to continue to operate for a few years** more since replacing them would require a re-design of the complete architecture requiring substantial cost and resource.

The problem is, to extend the useful life of these systems they often need to communicate with new computers or systems, over networks carrying different flows of information, but which may also contain malware. The first challenge then is to isolate them while restricting the communication to limited sources/destinations. The second is to ensure that any data transferred between these old and new systems can to be validated in a way that bad or malicious content can't be exchanged.

Old systems frequently lack security. The hardware or the operating systems, including the TCP/IP stack, may be old and not updated when new vulnerabilities are identified, such as the VXworks 'Urgent11' or attacks like 'Ripple20' affecting millions of IoT devices in June 2020. In these environments, the use of firewalls may not be sufficient, being software based and subject to compromise; Data diodes only allow one-way communication meaning that, due to the configuration of traffic flow, either updates can't be done, or business information cannot be retrieved. A visit to site is often the only way to resolve the issue in this case, requiring resources to make things happen, and capacity to do it quickly where delay might put care at risk if things take longer than expected.

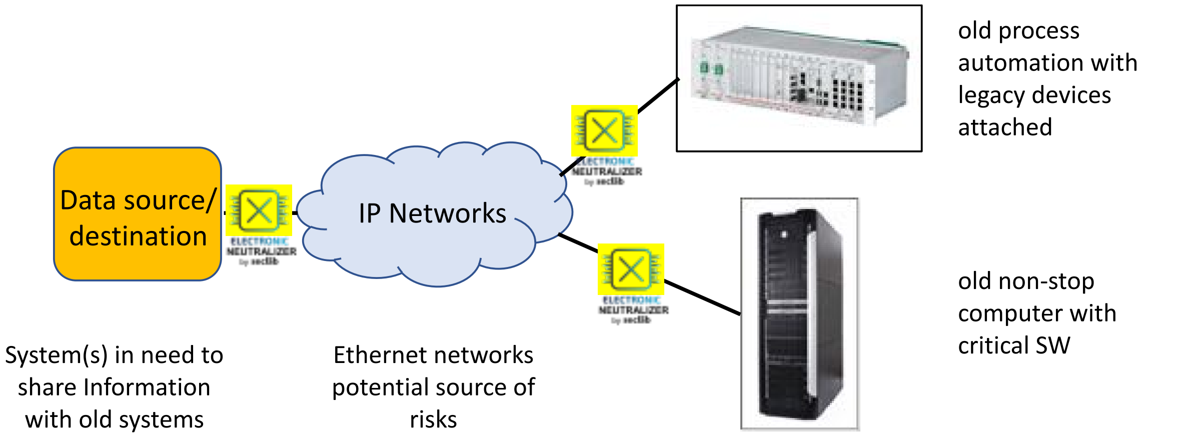
In short, the best option in these circumstances is "let's not change anything".


old process automation with legacy devices attached
Data source/ destination
IP Networks
old non-stop computer with critical SW
System(s) in need to share Information with old systems
Ethernet networks potential source of risks

The solution? inserting **SECLAB "Neutralizers"** near each end, whether inside or outside the Enterprise. Unlike 'Air Gapping', this option allows the networks to be connected by inserting a device that can't be compromised and lets only validated/certified content to be exchanged for a specific set of sources & destinations. The **SECLAB Secure Xchange Network SEC-XN** product range provides an **'Electronic Airgap'** which allows file exchanges or application data flow between two isolated network domains without creating a network route between gates.

The benefits? Legacy systems can be connected without any need for a patch at the OS or network level. Information exchange can be made inside or outside of the Enterprise and without the need for expensive and time-consuming site visits. The valid communication flow can be ‘hardwired’ or made possible for change. In summary:

- Extending the life of the investment
- Reducing the capex and opex requirements
- Increasing the level of security and reducing the risk



KEY FEATURES

Installation	• **Simple** and **fast deployment** requiring only two IP addresses. • **Automated maintenance** (encrypted & signed packages by Seclab)
Security	• Sustainability of **security policies guaranteed** by the fixed factory configuration in **electronic components**, without on-site configuration. • **Complete protocol segregation**: only the transferred file passes from one gate to another. • Immunization to network attacks with only one ANSSI certified appliance. • Protection against all low-level layer network attacks. • **Integrity** and **traceability of files** via signatures verification. • Rejection of files without digital signature or with invalid digital signature.
File Transfer	• **Bidirectional** or **unidirectional** transfer. • Gates in client mode or **FTP/ FTPS/SFTP** server. • **Tracing of transmitted files** (name, size, fingerprint). • **File filtering** via digital signature.

For more information: Please contact us at info@seclab-security.com, +33 4 11 93 08 59

(*) See https://www.immuniweb.com/blog/5-common-web-security-mistakes-that-costs-millions.html © 2020 ImmuniWeb

Contact

https://www.seclab-security.com

contact@seclab-security.com

@seclab_

/seclab

seclab