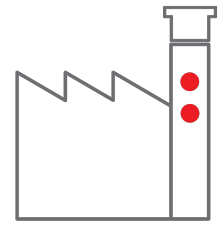
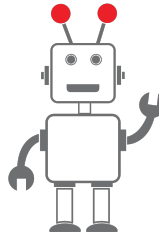


# Neuropil

Secure Interaction for Things



The exchange of data between applications continually raises concerns as to the authorization and dynamic network of devices. In particular, within the realm of IoT, some messaging paradigms are used which from a security perspective offer little to no value. Closed systems arise, yet the future data value remains unclear. Additional project and integrations costs are a direct result of delays in connections. Data quality, data transparency, and data sovereignty of users, companies, and organizations suffer as a result of this.

## **CHALLENGE**

What is Neuropil? We all have it in us: The fibrous network of tissue which forms the gray matter in our brain. Neuropil facilitates the networking between individual cells. It is in this manner that the Neuropil layer, an open source solution, assures the stable communication between machines and applications. What makes it so unique is that the secure exchange of data between the IoT devices and applications is dynamic, decentralized, and fully automated.

## **SOLUTION**

The Neuropil® layer , therefore, ensures data quality, data transparency, and data sovereignty all the while reducing IT costs, maximizing availability, and increasing reliability.

A secure IoT is a crucial prerequisite for secure collaboration and competitive businesses.

The Neuropil® layer provides:

- Automatic discovery of data channels across enterprises
- Attribute based access control to authorize data exchange
- Asymmetric end-to-end encryption between the participating systems
- Protection of IoT devices regarding excessive payloads
- High scalability without central infrastructure
- Centralized governance, but decentralized messaging

[www.neuropil.org](http://www.neuropil.org)  
[neuropil@pi-lar.net](mailto:neuropil@pi-lar.net)

V.i.S.d.P. Stephan Schwichtenberg  
pi-lar GmbH  
Gotenring 4  
HRB 81810  
50679 Köln