neomia pulse

Multi-Factor Authentication and User Behavior Analysis Platform based on Behavioral Biometrics and Contextual Analysis powered by Artificial Intelligence

Current challenges

The classical connection approach mainly based on static authentication (single or double factor), raises questions because how to certify that:

- Is the user the real trusted one?
- Is the user the same all the way long from login to logout?
- Is the data captured by a user, an automated process, or a robot?
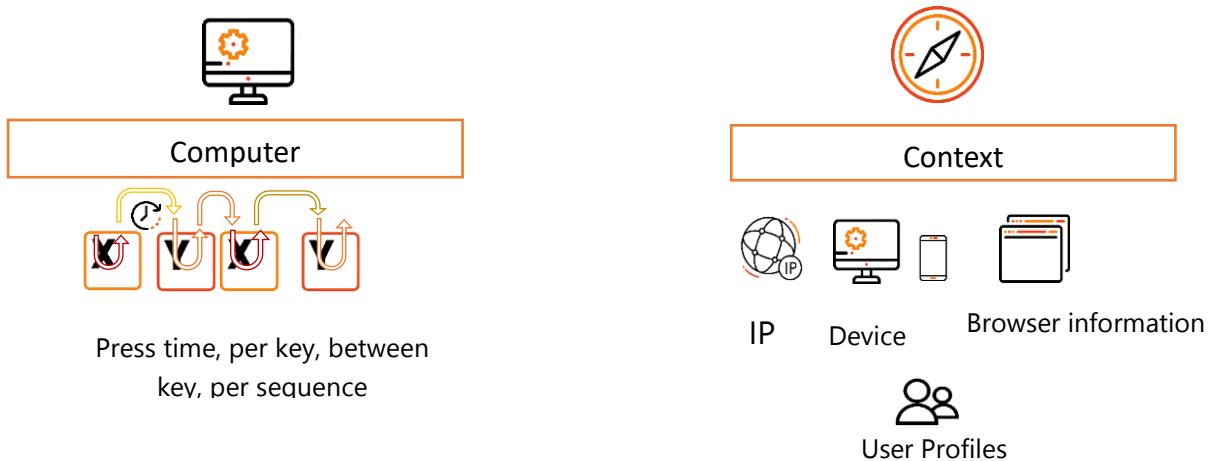- Is the used machine safe?

This approach cannot answer these questions because it does not detect either identifiers usurpation or compromise session.

Neomia Pulse innovative approach, powered by AI

neomia Pulse **seamlessly** and **frictionlessly** authenticates users, detects, and blocks suspicious activities through a combination of **behavioral biometrics** and **contextual analysis**.
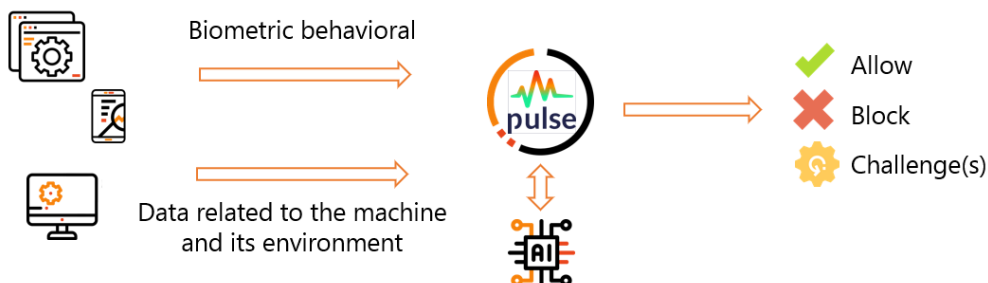
In real time **neomia Pulse** collect:

- behavioral data (mouse movements, typing cadence, swipe patterns, ...),
- contextual data related to the equipment used (physical, software, temporal, and geographical data).
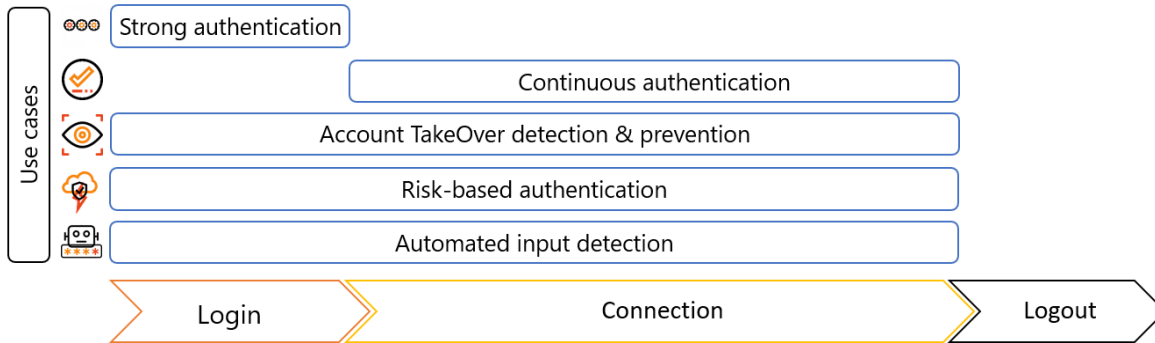

Computer

Press time, per key, between key, per sequence

Context

IP   Device   Browser information

User Profiles

Per user **neomia Pulse** built and defined :

- a DNA based on user's **trusted behavioral biometric** to prevent the use of spoofed credentials or to block spoofing attempts during a session,
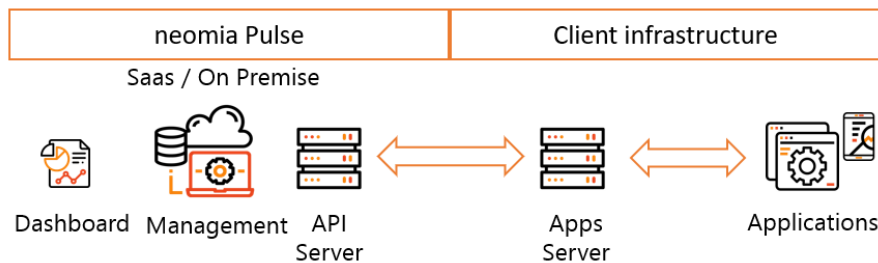- a risk level related to its hardware and software ecosystem.

Biometric behavioral

Data related to the machine and its environment

pulse

✔️ Allow
❌ Block
⚙️ Challenge(s)

neomia Pulse use cases

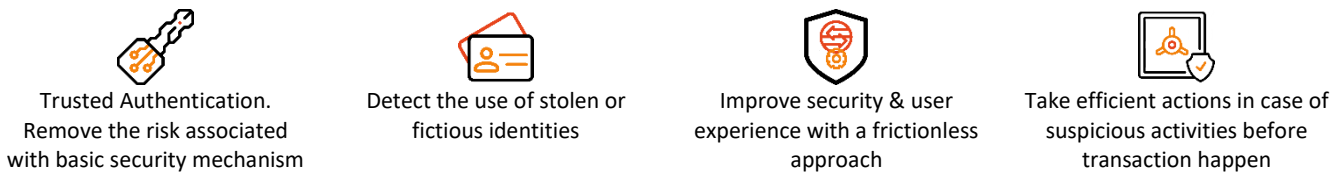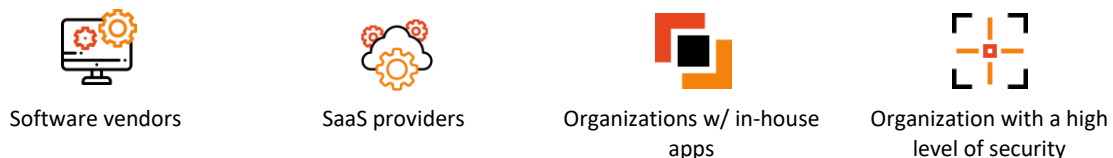| Use cases		
Strong authentication		
Continuous authentication		
Account TakeOver detection & prevention		
Risk-based authentication		
Automated input detection		
Login	Connection	Logout

neomia Pulse is easy to integrate

Into your applications and allows you to adopt a security policy at the design stage and instantly increase their level of trust

neomia Pulse	Client infrastructure
Saas / On Premise	

Dashboard Management API Server   Apps Server   Applications

neomia Pulse allows to

Trusted Authentication. Remove the risk associated with basic security mechanism

Detect the use of stolen or fictious identities

Improve security & user experience with a frictionless approach

Take efficient actions in case of suspicious activities before transaction happen

Neomia Pulse serves a wide panel of industries and is aimed at any organization

Software vendors

SaaS providers

Organizations w/ in-house apps

Organization with a high level of security

neomia Pulse, to discover it

To discover the power of **neomia Pulse** and its ease of use, we offer you:
- ➢ a complete online demonstration environment, both on the user and manager side,
- ➢ to test it in your ecosystem through a proof of concept with strong support from us.

Do not hesitate to contact us!

3 Rue Paul-Henri SPAAK,
68390 SAUSHEIM - France

neomia

contact@neomia.ai
03 89 33 58 20