neomia pulse

Identity Control & MultiFactor Authentication IC-MFA

Behavioral Biometrics & Contextual Analysis powered by Artificial Intelligence

Cybercrime and data theft are increasing daily. Companies and public organizations are prime targets. It has never been more important to **prevent large-scale security risks, starting with the basics: the identity.** This is an extremely difficult task, given the wide range of professions, uses and locations of employees.

Current challenges

The current situation is mainly based on simple authentication (login, passwords), sometimes reinforced by an MFA system, which essentially relies on tokens or physical devices.

It is very difficult to maintain concurrent security policies that combine a high level of security and address all use cases.

Identity verification can be carried out in two different sequences. The login phase, and the monitoring when critical actions are performed.

Biometric identity verification is the most resilient of the 3 authentication components (what I know, what I have, what I am). To meet the challenges of universality, user acceptance, ease of deployment and cost, it is important to provide biometric identity capabilities, without devices or tokens.

Solutions must provide simple answers to the following questions:

- Is the connected user the legitimate user?
- Is the user the same throughout the connection?
- Is the data entered by a user, by an automated process or a robot?
- Is the machine used risk-free?

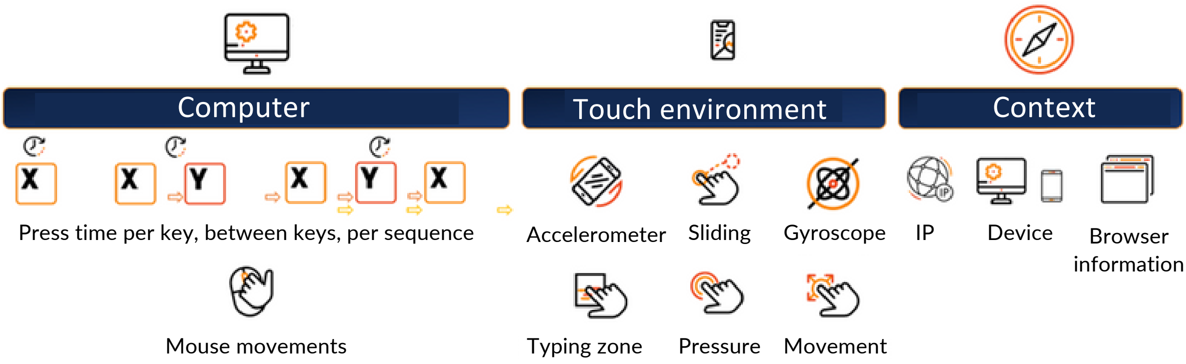
The approach must leave no doubt regarding the possibility of identity theft or session corruption.

neomia Pulse, an innovative approach powered by Artificial Intelligence

neomia Pulse seamlessly and without friction authenticates users, detecting and blocking suspicious activity through a **combination** of **behavioral biometrics** and **contextual analysis.**

neomia Pulse collects in real time:

- behavioral data (typing dynamics, mouse movements, touch screen use, etc.);
- contextual data linked to the equipment used (physical, software, temporal and geographical data).



Computer

Press time per key, between keys, per sequence

Mouse movements

Touch environment

Accelerometer

Sliding

Gyroscope

Typing zone

Pressure

Movement

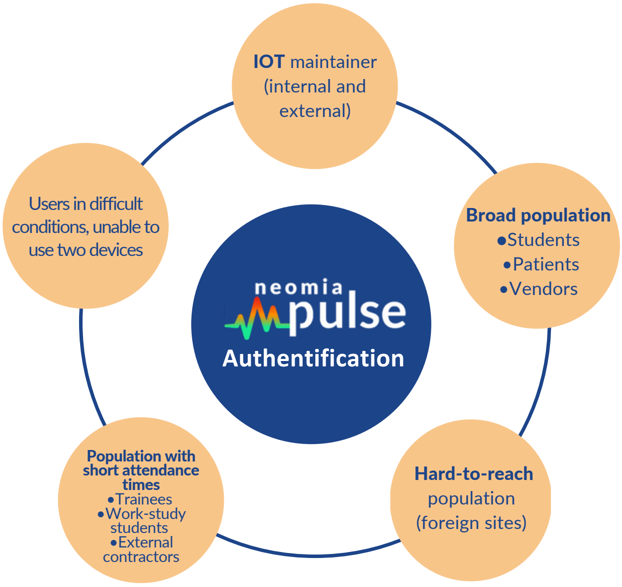
Context

IP

Device

Browser information

neomia Pulse, use cases



neomia pulse Authentification

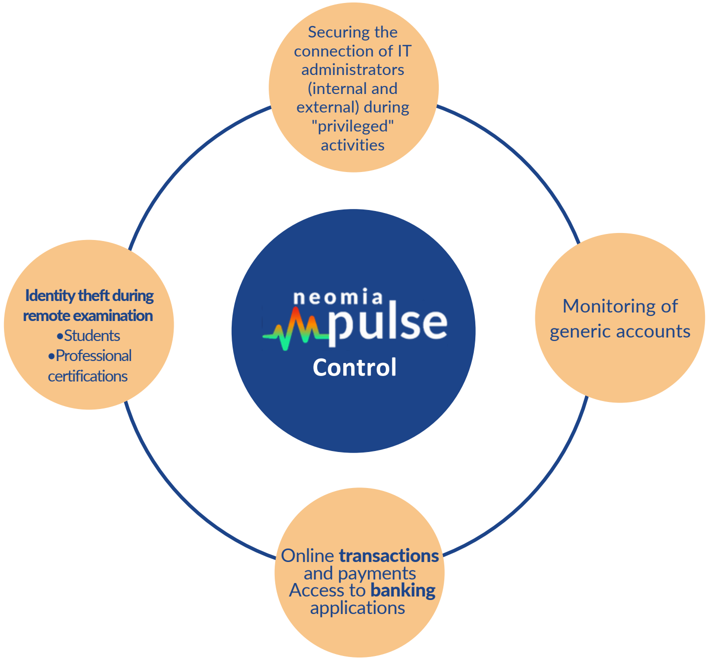
IOT maintainer (internal and external)

Broad population
- Students
- Patients
- Vendors

Hard-to-reach population (foreign sites)

Population with short attendance times
- Trainees
- Work-study students
- External contractors

Users in difficult conditions, unable to use two devices



neomia pulse Control

Securing the connection of IT administrators (internal and external) during "privileged" activities

Monitoring of generic accounts

Online **transactions** and payments
Access to **banking** applications

Identity theft during remote examination
- Students
- Professional certifications

neomia Pulse is easy to integrate

Pulse can be integrated at different levels

- API integration with your existing identity management systems.
- Pulse integrates the latest-generation SAML / OIDC protocols, for seamless connection to your IDP.

neomia Pulse allows to

Eliminate the risks associated with passwords and static authentication

Detect the use of stolen or fictitious identities

Improve security and user experience with a continuous, frictionless approach

Define and implement effective measures in the event of suspicious activities

neomia Pulse is designed for all types of organizations

Software vendors

SaaS providers

Organizations with in-house applications

Operators of vital importance

neomia

3 Rue Paul-Henri SPAAK, 68390 SAUSHEIM
contact@neomia.ai
☎ 03 89 33 58 20