
neomia
pulse
Identity Control &
MultiFactor Authentication
IC-MFA

neomia Pulse

Identity control
the first security barrier for IT/OT access

"Protecting this connection between identities (employees, contractors, partners, machines) and technology seems quite complex to manage properly when you stack it all up" **JDN**

"Identity monitoring is a prerequisite for the quality and security of healthcare." **ARS Bordeaux**

"Identity: A new front line for security in a digital world": **Last Pass**

So, at some point, we're going to have to become coercive. No more access without MFA, no more VPN provider accounts without monitoring or open to the whole world 24/365, no more remote, external, unfiltered control..... **DSIH**

Trend 1: Human-centric security design
Recognizing that traditional cybersecurity awareness programs have failed to reduce unsecure employee behavior, Gartner is calling on CISOs to take new approaches by reviewing past incidents to better identify frictions. **The aim: to ease the burden for employees by adopting more human-centric controls and retiring controls that add friction without meaningfully reducing risk.** .... **GARTNER 9 human-centric trends of cybersecurity in 2023**

pulse

neomia

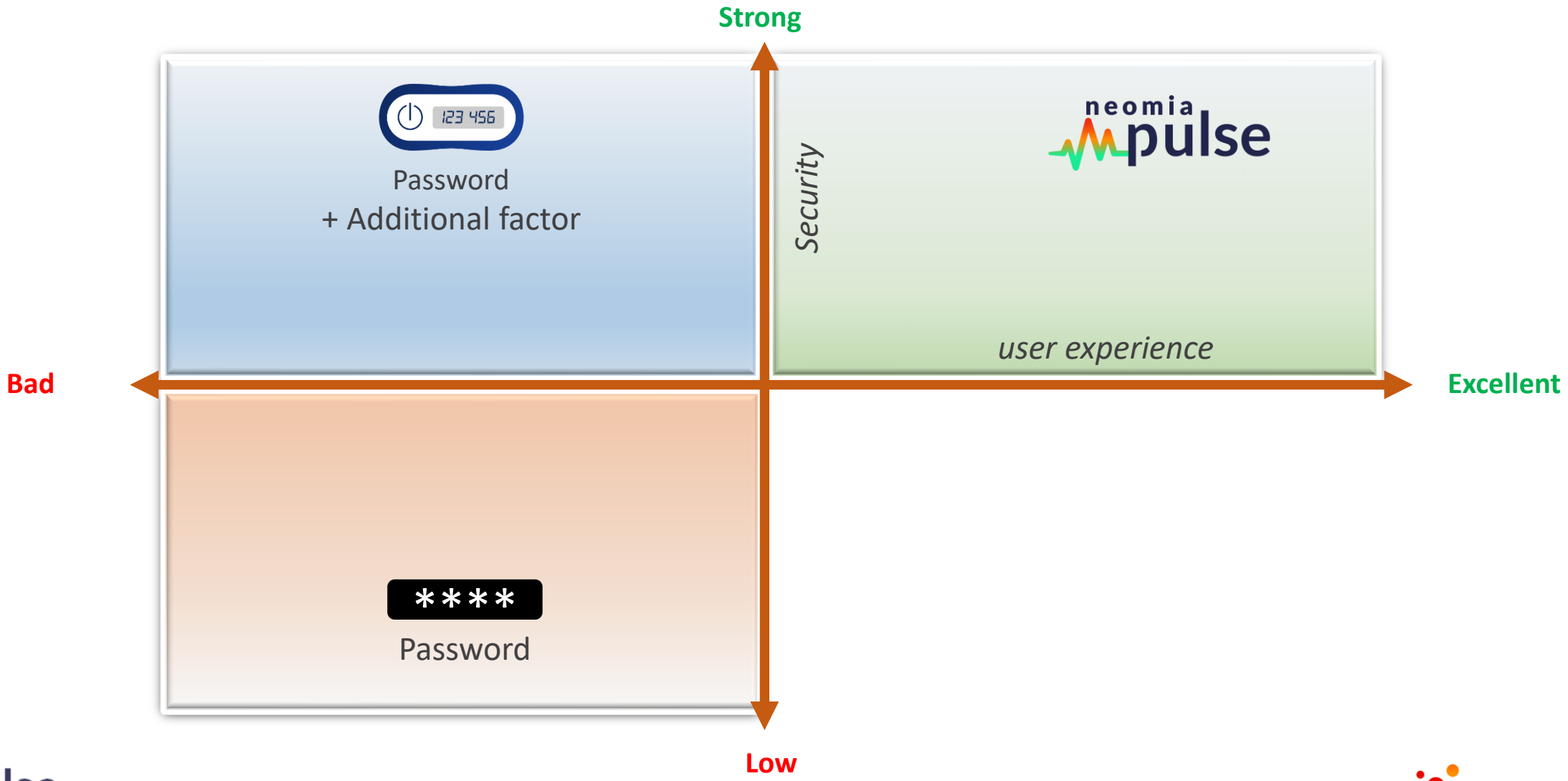
General reminder: Categorization of authentication factors

(ANSSI: "recommendation relative to multi-factor authentication and passwords": chapter 2.4)

pulse

neomia

MFA: Authentication factors quadrant



Pulse: Application domains

Secondary authentication: Application opening	Available
Targeted authentication: On demand in an application (process security)	
Primary authentication Opening the operating system of a computer (connected)	Available under certain conditions
Multiple authentication: Log on to generic accounts	Available under certain conditions
Continuous authentication: Continuous authentication throughout the session	Available Q4 2023

Already prepared for the future: passwordless

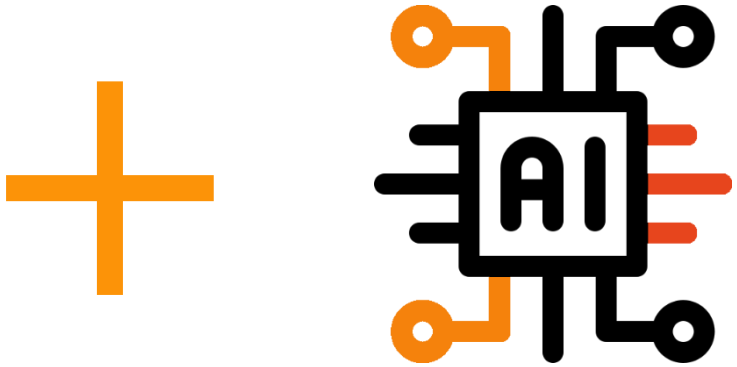
pulse

neomia

Pulse: Transparent, frictionless authentication!

First and foremost, it uses standard hardware

coupled with AI algorithms (developed in-house)



This allows a

transparent authentication:
- the strong authentication factor is invisible to the user,
- he only "sees" the first factor (login credential)

frictionless authentication:
- users don't need to use, manage or worry about an additional system

pulse

neomia

neomia Pulse

How does it work?

MFA: The current situation

Solutions based on physical tokens / certificates etc...
They require the presence of devices, with their associated problems

- Park management (access, obsolescence, deprovisioning, etc.)
- Can be lent or stolen, etc.
- Costs

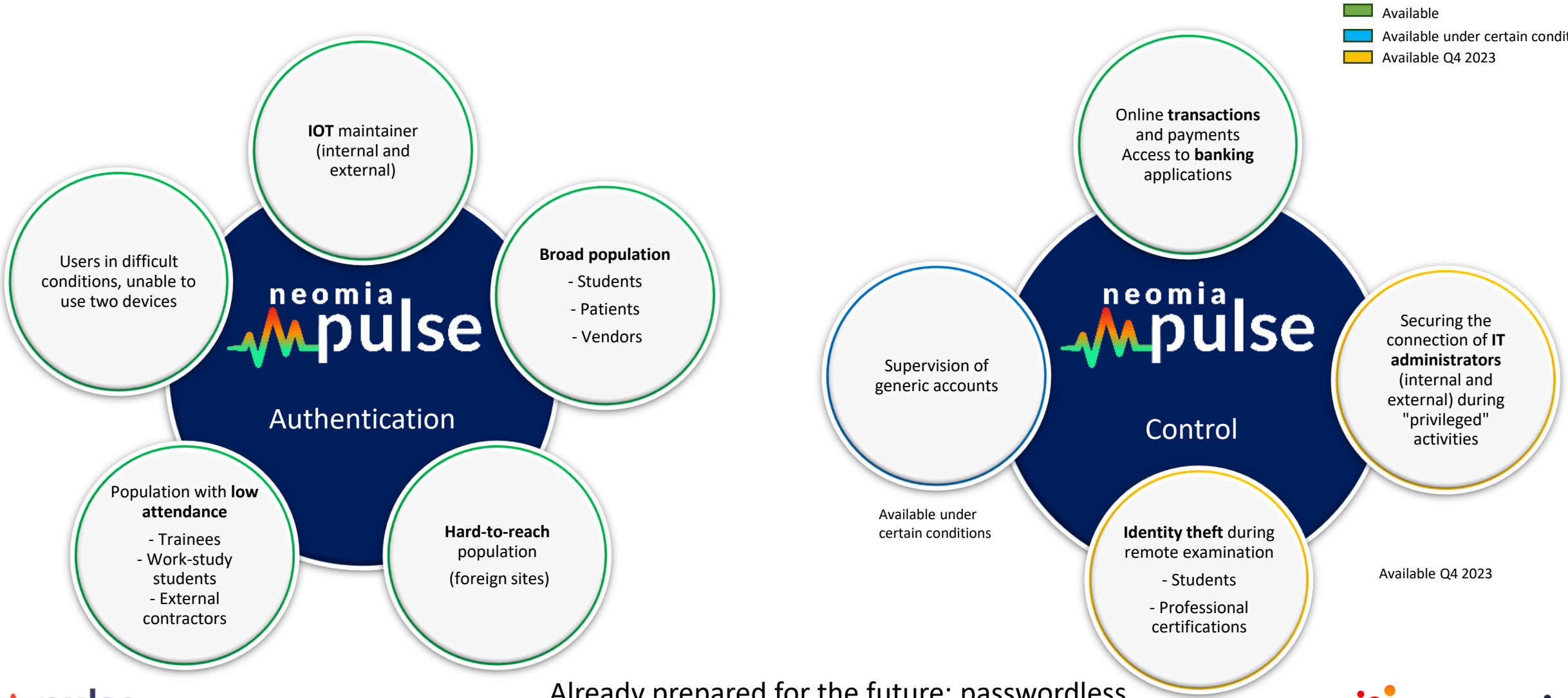
Neomia pulse: technical elements and context

Control type	Control impact	Population type	Use type
AI-based strong authentication	**Full** validation	**Everybody**	• **Permanent** • Over **specific periods** E.g.: Distance learning students
Authentication strengthened by analysis of **contextual criteria**	**Continuous** control validation	**Segmentation** by business profile • Roaming users • Privileged users • Users of a specific application • …	
Automated input detection with the possibility to **impose a challenge**	**Targeted** validation (related to a specific software action)		
Blocking the use of a usurped account			

pulse

neomia

Use cases: use cases...

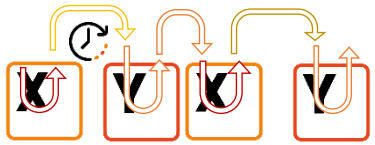


Already prepared for the future: passwordless

Technique: general operation

For each user, **neomia Pulse** generates **unique fingerprints** based on **behavioral biometric data** and **contextual analysis**

Computer



Press time per key, between keys

Context

IP Device Browser information

User profiles

Note: Neomia Pulse **does not collect** the characters entered by the user

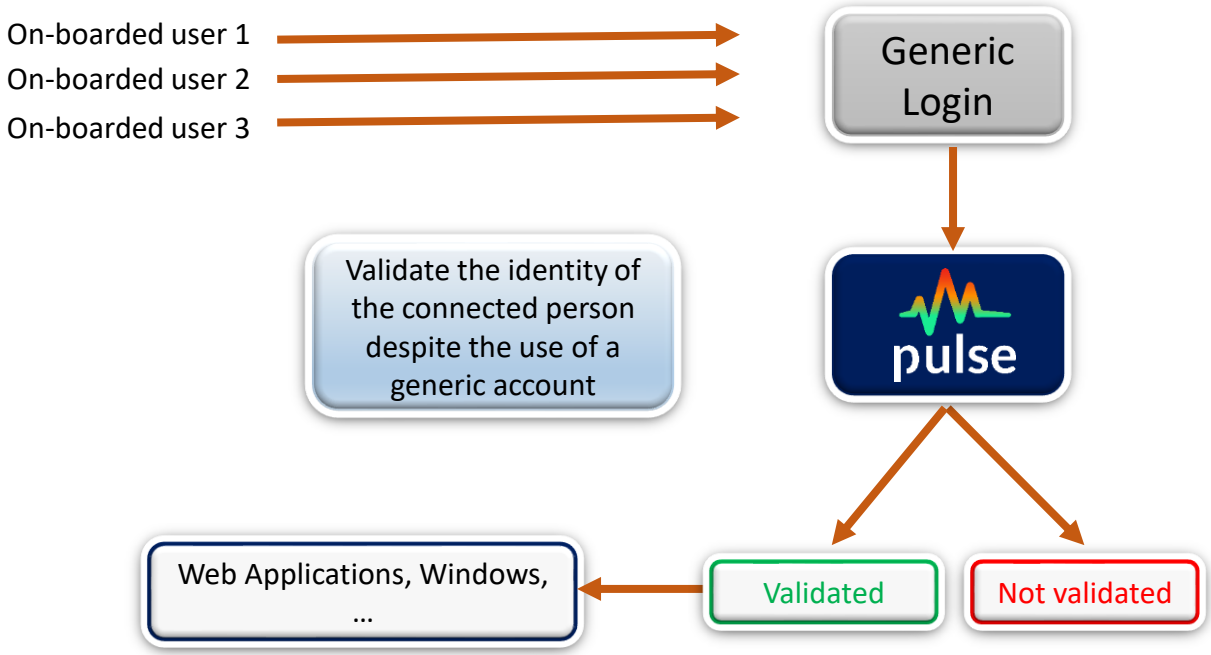
pulse

neomia

Focus on use cases: the famous generic accounts ...

For various reasons (history, ease of use, etc.) generic accounts can be used, with associated risks:

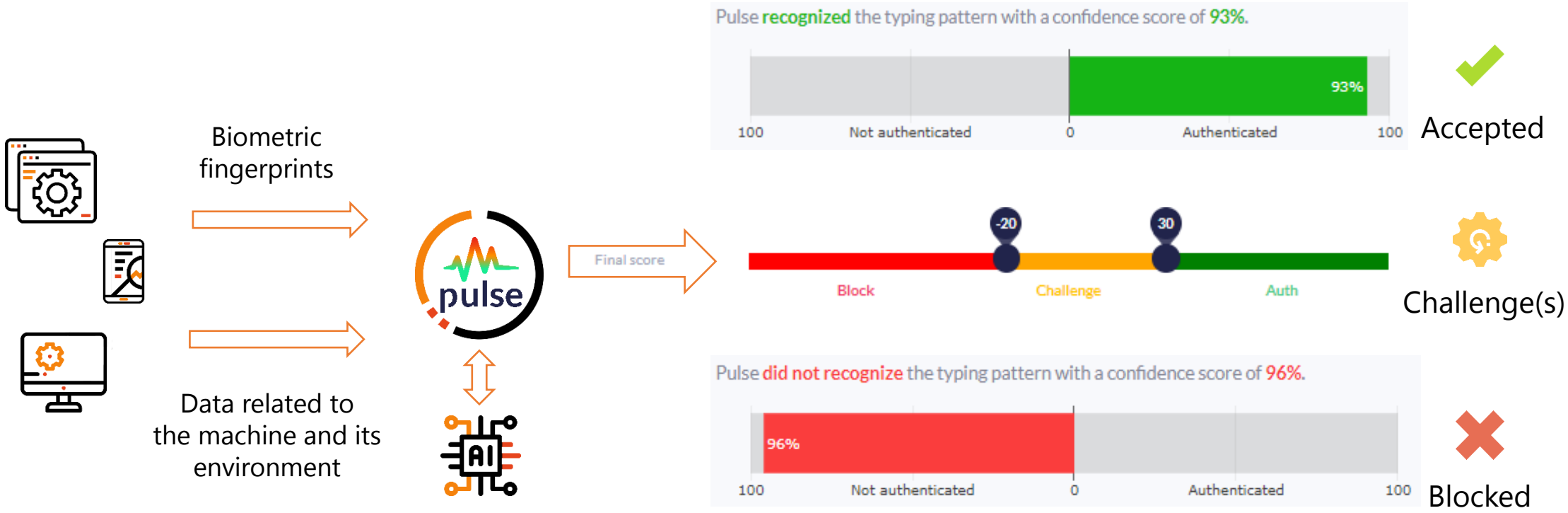
- Lack of identity control;
- Risk of these accounts being used by non-legitimate persons without any possible detection;
- Dissemination of these accounts by internal and/or external parties (partners, service providers) without any possible control;
- …



Technique: understanding the scoring

It allows to **compare biometric fingerprints** generated **dynamically** at each connection with **reference behavioral biometric fingerprints**

Definition of a **trust** or **mistrust** **index**, potentially reduced by the **level of contextual risk**



2 Options Block status:

- Re challenge
- Immediately block an account if it is certain that it is the wrong person

Integration: Native via API

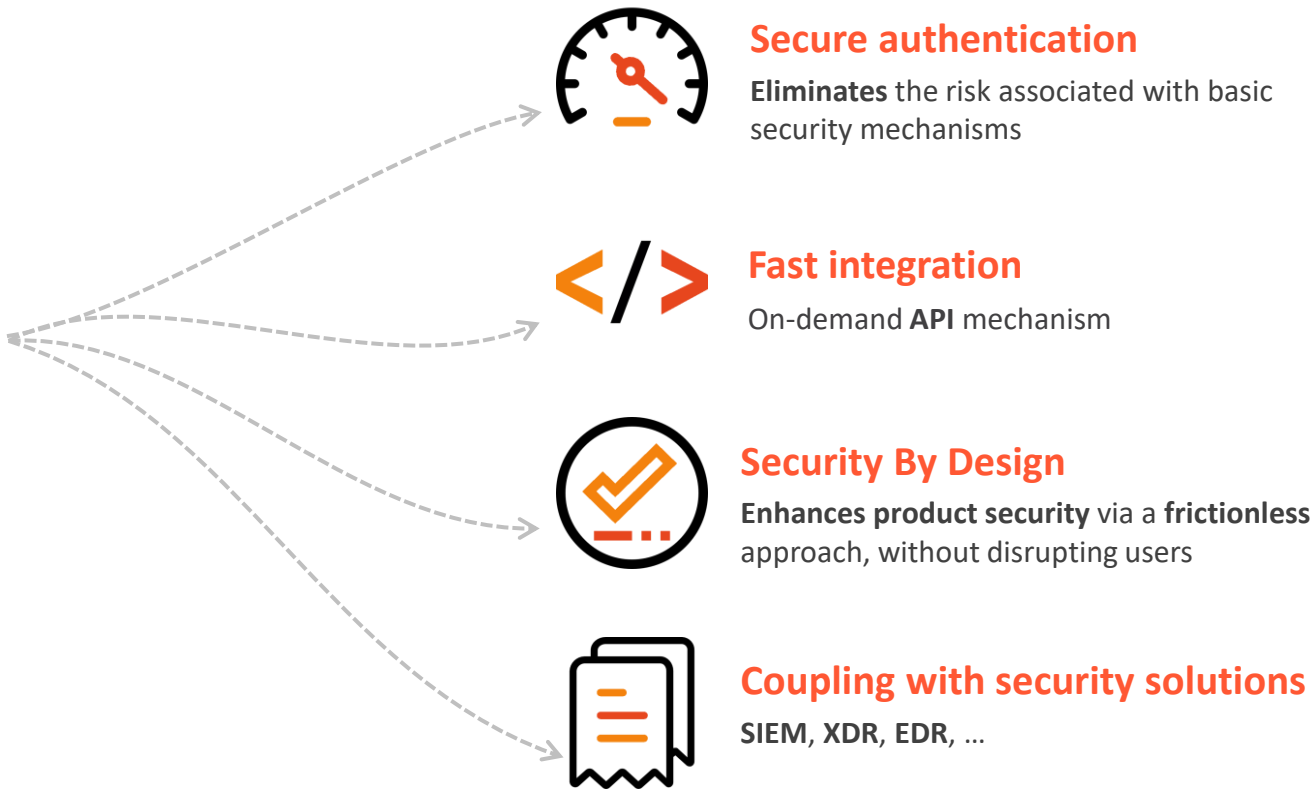
Neomia Pulse helps developers, DevOps and DevSecOps engineers to secure their applications.

Our **integrated API** system allows them to adopt a Security-by-design policy at the core of their own applications and instantly improve the level of trust.

Software vendors

SaaS providers

Organizations with in-house applications



Secure authentication

Eliminates the risk associated with basic security mechanisms

Fast integration

On-demand **API** mechanism

Security By Design

Enhances product security via a **frictionless** approach, without disrupting users

Coupling with security solutions

SIEM, XDR, EDR, …

pulse

neomia