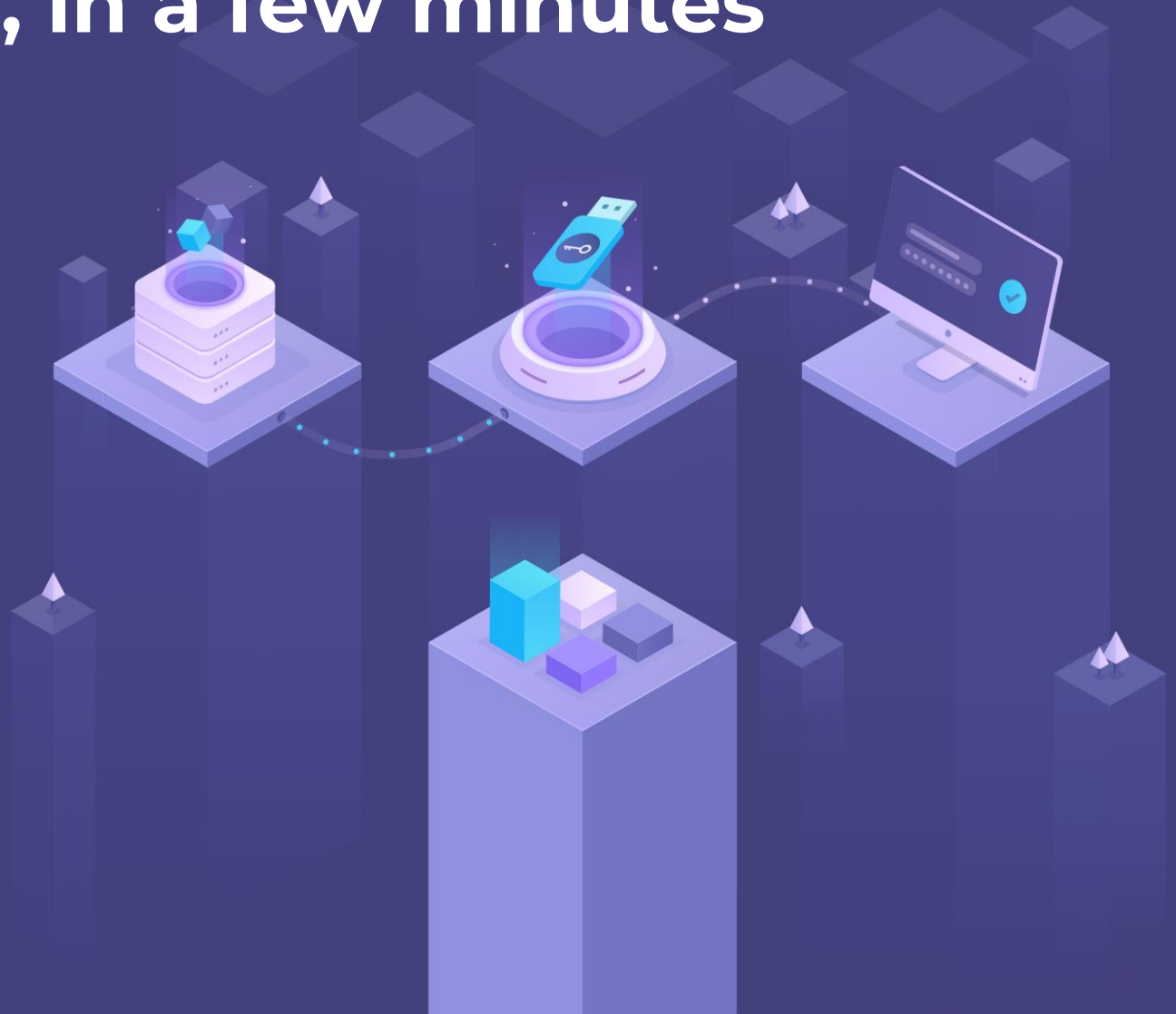
MFA in all applications, in a few minutes

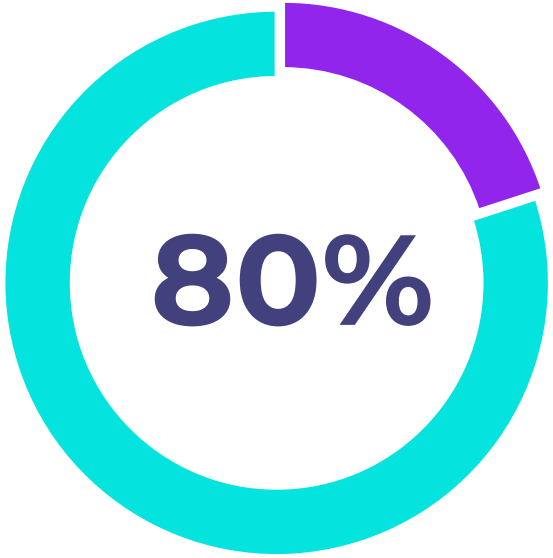
Krzysztof Góźdź, krzysiek@secfense.com
Aleksandar Brdar, aleks@secfense.com



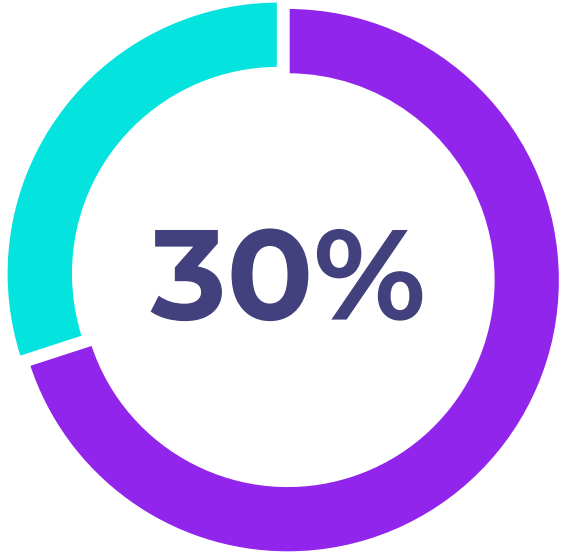
SECFENSE

SECFENSE

The data is clear



Incidents begin with an account takeover



Intrusion comes from inside the organization

SECFENSE

Strong authentication in all applications!

DORA

Article 8

Protection and Prevention

4. As part of the ICT risk management framework referred to in Article 5(1), financial entities shall:

(d) implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated controls systems to prevent access to cryptographic keys whereby data is encrypted based on results of approved data classification and risk assessment processes;

NIS 2

Article 21

Cybersecurity risk-management measures

2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

SECFENSE

Strong authentication in all applications. How to implement them?

Traditional approach - modification of all applications

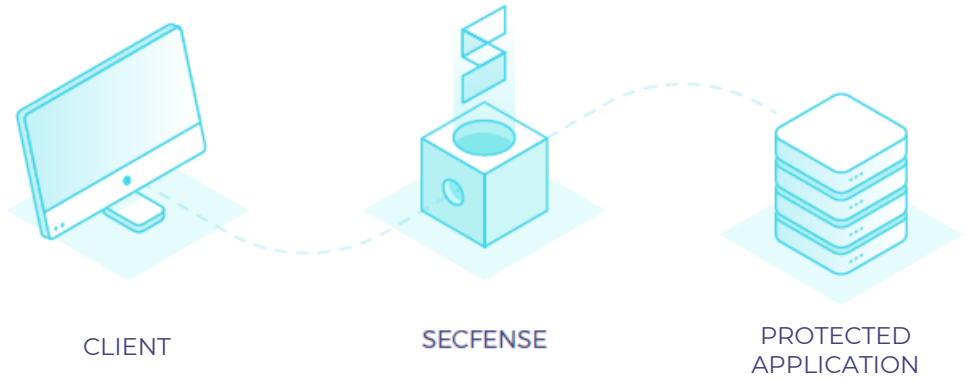
- Persons?
- Vendors?
- Technology?
- Time?
- Risks?

Secfense solution – broker-based

- No modifications of protected applications
- Quickly and easily
- On a massive scale
- In a comfortable way for users

SECFENSE

How it works?



Administrator:

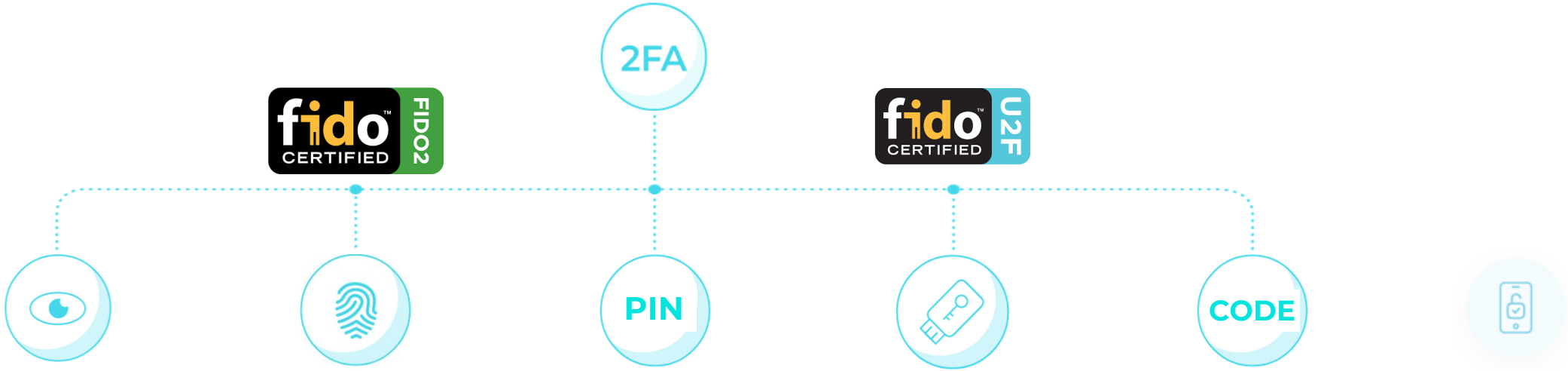
1. Installation of hardware, software or use of the "cloud" service
2. Redirecting network traffic to the application
3. Automatic learning how to login to the application

Users:

4. Select, add and use a second authentication factor

SECFENSE

Any second factor



Demo