

Flexible Identity Authentication

Easily Secure Connections

Today, 80% of data leaks are induced by password use. Security and access management, however, tend to grow more complex as they evolve. Passwords seem to be inducing risks, which lead them to fail as relevant security features.

They cause trouble to the users who may need keep in mind too many passwords (40 per person on average). These users often lose ground considering their complexity. Also, passwords indirectly make CISOs' work much tougher, as they must secure accesses and strengthen security.

The current context sees remote access become mandatory: companies must then ensure data protection while simplifying their users' daily life. Flexible Identity Authentication is an effective security solution enabling you to:



Secure access to company resources:

- Mobile users
- Partners
- Company's IS
- Cloud services



Respond to regulatory requirements:

- Personal and health data
- Credit card or payment details subject to the PCI-DSS standard
- SCADA-type industrial networks



Prevent identity theft:

- Prevent data theft
- Ensure Business Continuity



Control costs:

- No password means fewer tickets for your helpdesk to deal with
- Pay-per-use, regardless of the number of applications (fixed cost)

How does this solution solve the password problem?

Passwords-related threats aren't considered often enough; and, helpdesk interactions are often time-consuming. Through providing adaptive access policies based on scenarios, multi-factor authentication and Single Sign-On, Flexible Identity Authentication makes passwords disappear, while enhancing your security.

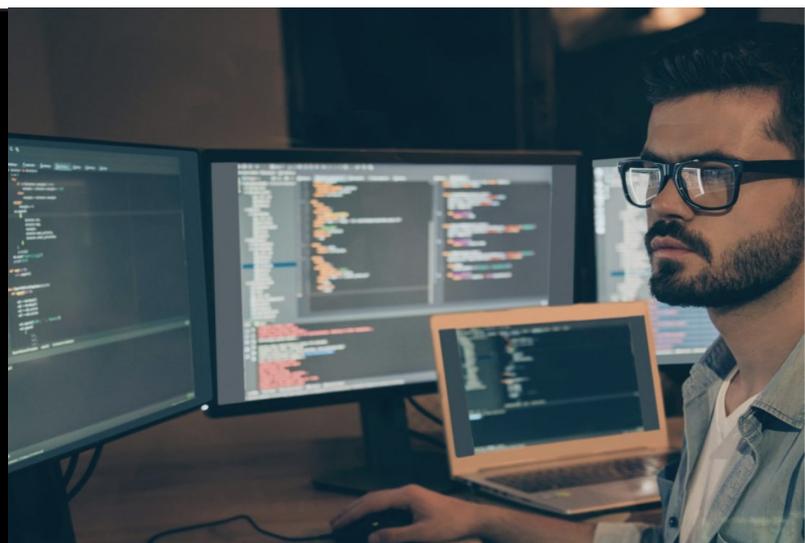
40%*

of helpdesk calls regarding passwords

62%*

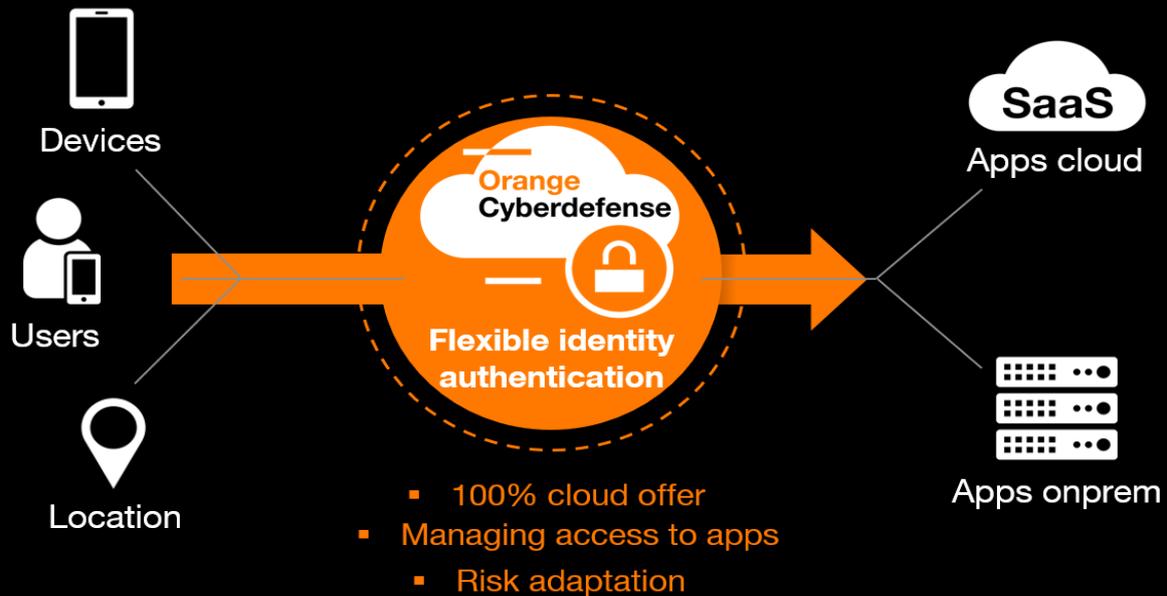
of users with similar password for multiple accounts

*Helpnetsecurity2020



Flexible Identity Authentication

Strengthen access security while improving user experience



What we offer

A wide range of user profiles-relevant tokens to choose from

- Physical tokens
- Software (computers, tablets and smartphones)
- Out-of-band SMS code sent by phone

Integration with more than 100 solutions

High compatibility with your hybrid applications: VPN gateways, virtualization solutions, on-premise and Cloud applications, etc.

Easy and instant management of user licenses

- Manually, through the administration portal, with possible import of CSV files
- Automatically, thanks to the Active Directory and solution synchronization

Granular security policy and single identification

A flexible, risks-based access policy matching your login environment and Single Sign-On (SSO) to streamline navigation processes through your Cloud applications.

Why choose Orange Cyberdefense?

- Solution available within a month, with no infrastructure costs and as a pay-per-use service
- Simple user interface and administration portal
- Adjustment of security policies based on ongoing evolutions
- Automatic deployment of secure authentication means
- 24/7 service: continuous monitoring of alarms and logs



For more information check www.orange cyberdefense.com

Contact us : info@orange cyberdefense.com