POSITION PAPER

Identity verification for remote employees

IDEMIA

Remote working: a major organizational shift

The trend towards a mobile, distributed workforce is accelerating, and an increasing number of employees are working outside of traditional office spaces, whether it be at home or on-the-go.

Remote working can be beneficial for employees, as it allows for increased flexibility and better work-life balance. For some organizations, remote work enables them to keep their businesses operating during times when office work poses a risk.

To fully enable a productive remote workforce, organizations need to ensure that the remote work experience is convenient and smooth for employees, while making sure that systems and data remain secure.

Identity verification can support remote work environments in a variety of ways:

Trust remote employee identities

Gain assurance that your known employee is the same person as the one who is working remotely and accessing critical resources

Hire and onboard remote employees

Enable both the new hire and the HR team to complete identity verification while working remotely

Enable a BYOD strategy

Adopt a bring your own device (BYOD) strategy into a corporate network, while maintaining its security

Secure access and transactions

Protect organizational resources and transactions such as account recovery, issuance and reset of WFH (Work from Home) credentials, or VPN access

Provide self-serve IT services

Enable workers to easily manage their own access credentials from onboarding to password reset

Organizations need to ensure that the remote work experience is convenient and smooth for employees while making sure that systems and data remain secure.

Key facts

73%
of all corporate departments will have remote workers by 2028[1]

$1,6 million
average cost of an insider attack to an organization[2]

77 days
average time needed to contain an insider attack[3]

X3
frequency of insider attacks have tripled since 2016[3]

Sources

[1] The 2020 Alcohol E-Commerce Playbook from Rabobank

[2] https://www.forbes.coqm/sites/thomaspellechia/2020/04/09/the-pandemic-may-provide-the-stimulus--e-commerce-alcohol-sales-have-needed/#6e614651b193

[3] EgamingReview,

[4] National Trading Standards UK

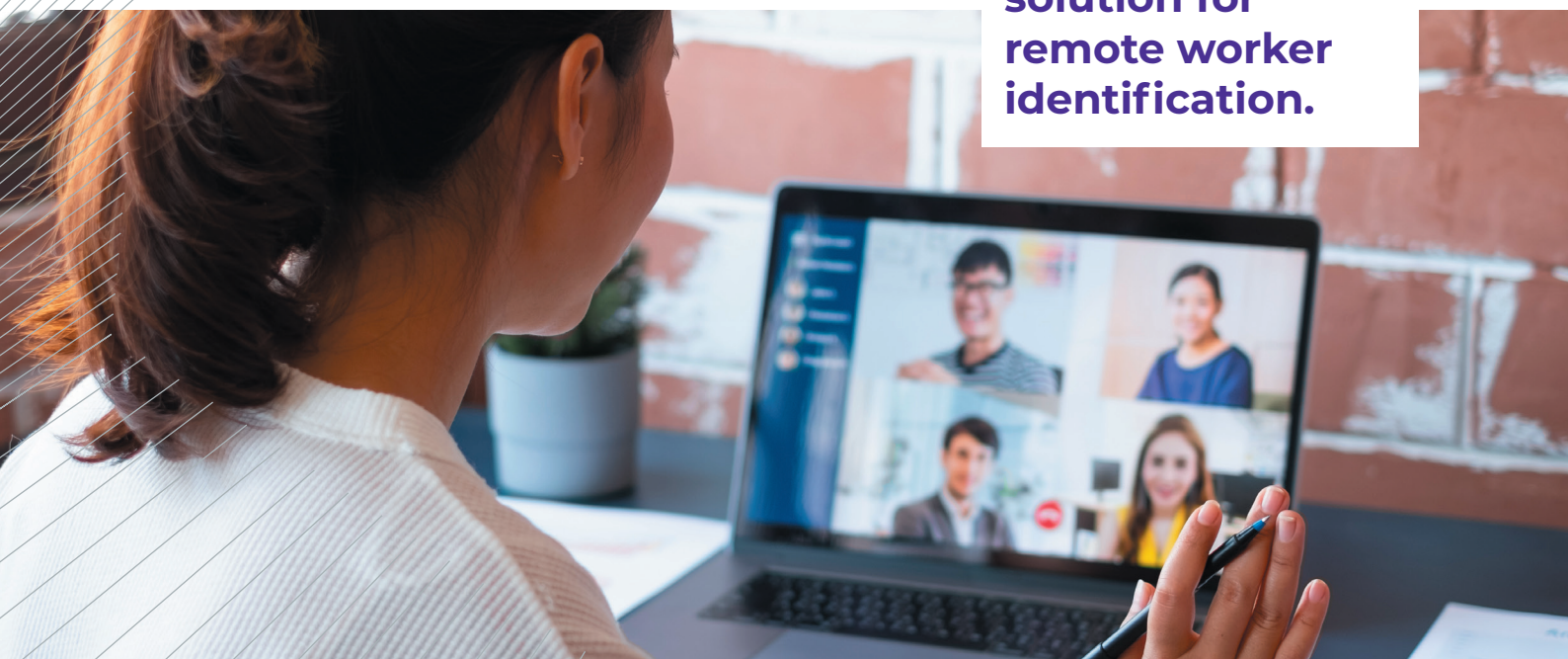
Identity: the challenge of remote work

The acceleration of remote work practices has opened companies up to unique security challenges:

- Correctly identifying remote employees and new hires
- Preventing unauthorized access to network and critical resources
- Verifying the identity of employees connecting remotely for the first time with their own device
- Preventing impersonation and unauthorized delegation of work
- Securing high-risk transactions, such as money transfer or reset of login credentials
- Ensuring data privacy and integrity
- Streamlining access and security protocols
- Controlling IT time and costs

A secure and convenient method of verifying remote employees is central to each of these challenges.

Identity verification provides a scalable and cost-efficient solution for remote worker identification.



Trusted digital identities for remote employees

Identity verification provides a scalable and cost-efficient solution for remote worker identification. It can help to:

Secure access and data

In a fully remote work environment, securing access and data is challenging due to the increase in identity theft and fraud. Identity verification ensures that only authorized employees have access to critical resources and can perform high-risk transactions.

Simplify onboarding

Remote identity verification simplifies the onboarding process by allowing companies to verify and trust the identity of a new hire or of a known employee connecting remotely for the first time

Enroll new devices

When remote employees use their own device for the first time, a trusted digital identity can be used to authenticate the user and enroll their devices.

Enhance efficiency and reduce costs

Reduce IT costs and resources needed to for identity lifecycle management, such as employee onboarding and account recovery.

Identity verification solutions

Designing a secure, compliant, and seamless identity verification solution involves a variety of different means such as:

ID documents

Employees and remote workers can use their smartphones to capture their ID document, passport, or driver's license.
The data is then verified for authenticity – with a trusted third-party or a root of trust.

Selfie

Remote workers can use their smartphones to capture a selfie and perform a liveness detection test. The selfie is compared with the portrait from their ID document and optionally with a root of trust.

Mobile 2FA*

The employee's mobile device is used as a trusted authentication device, associated with biometrics or PIN code, for an omni-channel experience.

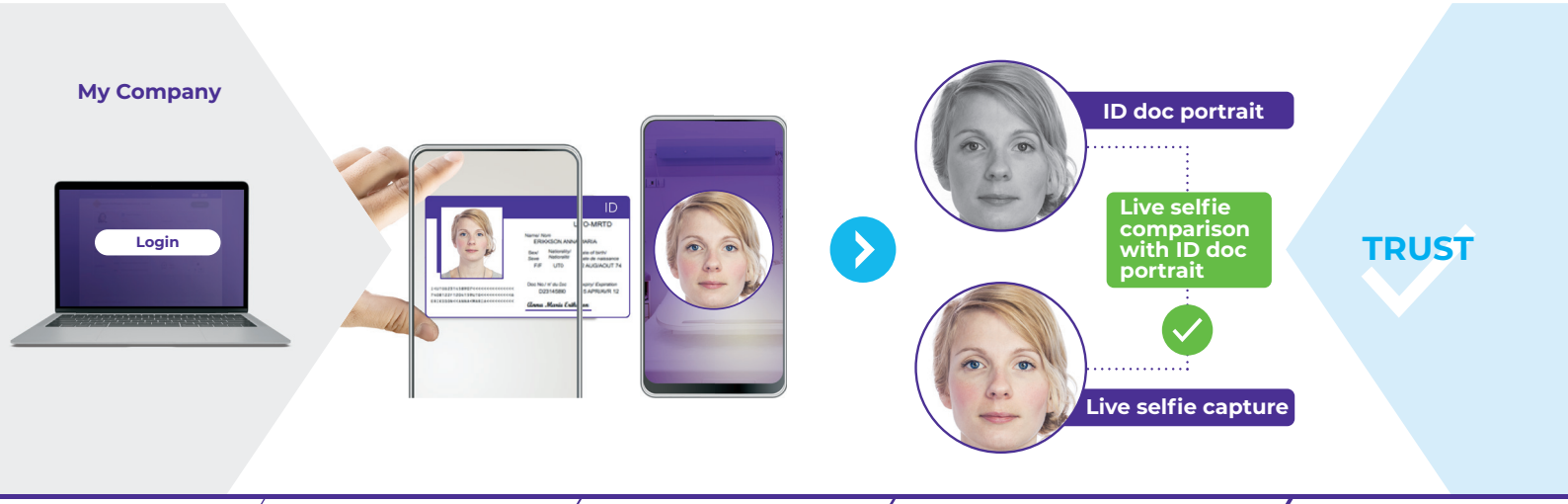
Risk-based authentication

The organization can automatically adjust the authentication requirements based on the risk score and its IT policies. For example, in high-risk instances, a user's biometrics can be requested along with a one-time password.

IDEMIA

Use cases

Employee ID proofing with ID scanning



Employee logs in using their own device

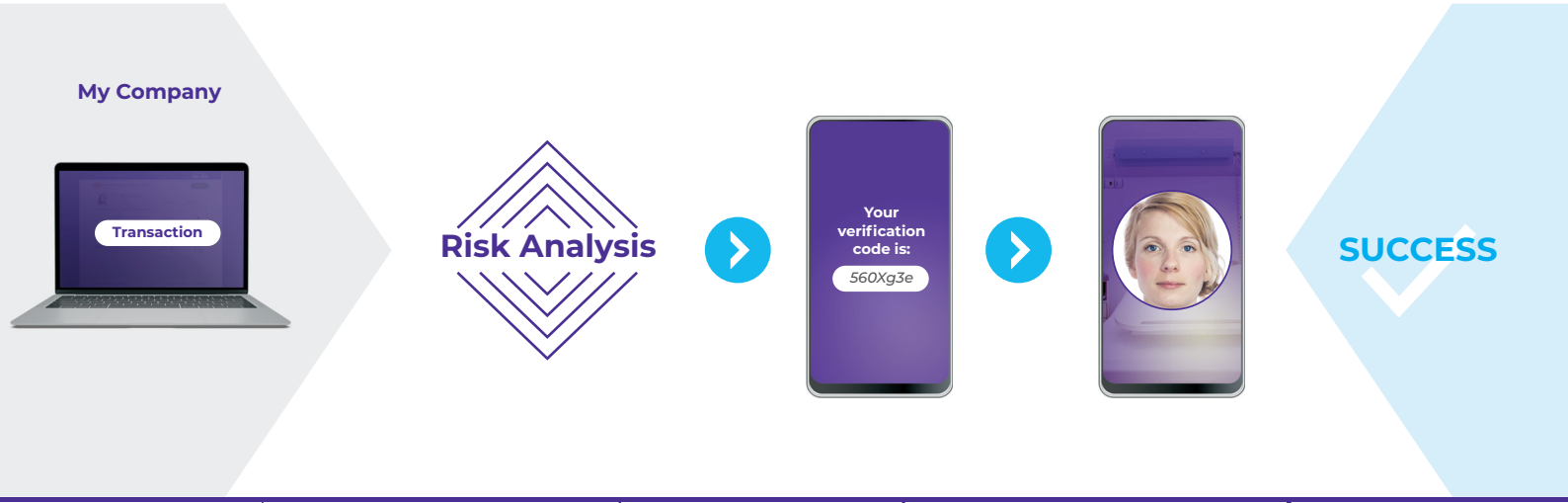
Employee scans their ID doc

Employee captures their biometrics

Biometrics verification

Employee's identity and device are trusted

Employee Authentication



Employee initiates a high-risk transaction

Context and risk are analyzed, triggering two-factor authentication

Employee gets a one-time password

Employee does a selfie check

Transaction is completed

We are **Digital**

idemia.com/**we-are-digital**

To learn more about identity verification for
remote work, or to schedule a demo, contact:
digitalid@idemia.com

IDEMIA

Join us on

www.idemia.com