>the_kernel / We don’t panic

PROTECT. DEFEND. SECURE.

>the_kernel

The Kernel has kept organizations safe for over **30 years** and prevented more than **35,000 cyber attacks**... and still counting.

We've secured organizations and built **trust** for both the workforce and customers.

30+
Years in the industry

7
Offices around the world

65+
Products

78
Partners across MENA

In-house **SOLUTIONS**

We've designed a suite of security management systems that takes care of your authorization and encryption needs for a secure operational process.

Identity Management

Cross-network data restriction system for authorized personnel only.

Cloud Security

Framework of services to protect cloud-based data.

Strong Authentication

Layered authentication system for a more secure access.

Public Key Infrastructure

360-encryption and decryption solution for sensitive digital data.

Partner **PRODUCTS**

We represent global cyber security names to provide you with class-leading authentication solutions that guarantee identity security.

yubico

gluu

secmaker

Authentication

Digital verification products you need

>

Control the access.
Protect your data.

Fortify your first layer of digital protection with industry-grade authentication products by the most trusted names in cyber security.

yubico

gluu

secmaker

yubico

>

yubico

Just ‘touch’ and **go**

Yubico is a Swedish cyber security company who pioneered the use of USB and NFC-based authentication keys.

Extremely portable, you simply insert and ‘touch’ the keys to verify your identity.

Product range includes the YubiKey 5 Series, the Security Key Series and YubiHSM 2.

yubico

Protect your
digital world

YubiKey **5 Series**

This signature series boasts two-factor, multi-factor and passwordless authentication, and seamless touch-to-sign capability.

Supports FIDO2, U2F, Smart card, OTP, OpenPGP 3

USB-A, USB-C, NFC, Lightning

IP68 rated: dust tight and water submersible

Security Key **Series**

This series combines hardware-based authentication, public key cryptography, and U2F and FIDO2, along with USB and NFC capabilities.

Supports FIDO2 and U2F

USB-A, NFC

Designed to be the strongest and most durable security key to market

YubiHSM 2

This series combines hardware-based authentication, public key cryptography, and U2F and FIDO2, along with USB and NFC capabilities.

Supports FIDO2 and U2F

USB-A, NFC

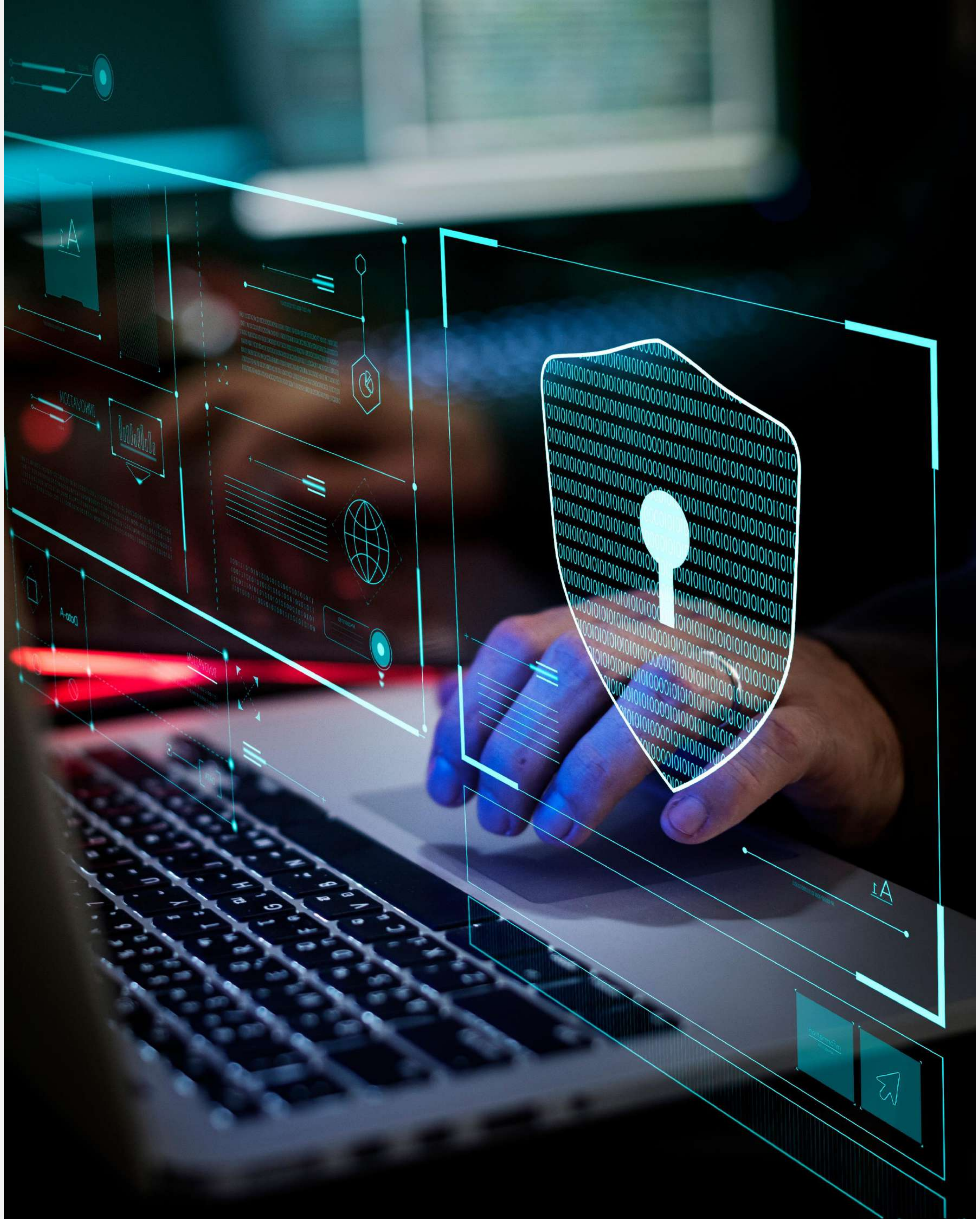
Designed to be the strongest and most durable security key to market

secmaker

secmaker

One card. One code. **That’s it.**

The Net iD Software Suite from Swedish security solutions provider offers a toolbox of several critical products for secure 2FA and MFA. All you need is a card; its corresponding code and you have access. It’s simple, secure, and fast.



>

```
elif _operation == "MIRROR_Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

    #selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
    #mirror_ob.select = 0
```

secmaker

Your toolbox for **passwordless logiN**

Standalone **PRODUCTS**

Net iD Enterprise

The Net iD Software Suite from Swedish security solutions provider offers a toolbox of several critical products for secure 2FA and MFA. All you need is a card; its corresponding code and you have access. It's simple, secure, and fast.

Net iD Portal

A user-friendly digital platform to manage your users' digital identities, whether its data collection and life cycle management or introduction of MFA and various function certificates. This innovative web portal also offers segmented interfaces for administrators, operators and users.

Net iD Access

Designed for secure mobile productivity, Net iD Access integrates with existing PKI infrastructure and supports both iOS and Android platforms. Choose between file certificates or a smartcard to implement the optimal IT security for your organization while allowing on-the-move access.

Net iD for Citrix

Log in faster to your Citrix environment. The Single Sign-On provides swift and simple and secure access to all your applications using a smartcard, mobile certificate or YubiKey and a PIN code.

secmaker

SOLUTIONS

Net iD OnPrem

Customize your protection levels based on individual requirements. Simply pick and choose the suitable components from the product suite to create your own security framework, while still running all the PKI architecture in your own environment.

SecMaker Live iD

Get protected faster; same security features but without the time and financial investment in hardware set-ups. This solution also allows cost-efficient scalability.

Net iD Public

Be part of a security collective and leverage an existing security framework. Offering shared security solutions, this is best implemented by organizations looking to provide national login and encryption services.

gluu

>

gluu

When you want scale, privacy and control

With its HQ in Austin, Texas, Gluu provides a centralized platform for the distribution and use of free open-source software for identity and access management (IAM).

>

gluu

Features

Single Sign-On (SSO)

Turnkey and custom systems to implement an organization and platform-wide authentication protocol.

Strong Authentication

Multi-layered authentication system to secure data and create a seamless collaborative environment.

Access Management

Control and implement security measures via a central platform, by defining access authorizations for both data and personnel.

Identity Management

Manage user data and information to grant privileges to systems and resources.

Directory Integration

Make Gluu your authoritative source of truth and sync directory servers to extend your existing identity infrastructure.

Fast Deployment

Linux packages for Ubuntu, CentOS, RHEL, and Debian make installing Gluu fast & easy on any cloud platform.

gluu

Customize your authentication management

gluu

Standalone **Products**

1 **Auth Server**
Based on the Linux Foundation Janssen Project, Gluu's Auth Server distributes open source software for IAM and its core uses including Single Sign-On (SSO), mobile authentication, API access management and 2FA.

2 **Casa**
Casa is a self-service digital platform which allows users to manage authentication and authorization preferences, view trusted devices, toggle 2FA functionality and even remove and replace 2FA credentials.

3 **Database**
A choice between LDAP and Couchbase, depending on the size of your organizational deployment.

4 **Shibboleth SAML IDP**
A must-have requirement to support SAML Single Sign-on (SSO).

5 **Passport**
An MIT-licensed, Express-based web application, Passport is used to enable social login, normalizing authentication and providing mapping for user claims.

6 **Admin UI**
User-friendly web interface for convenient configuration.

gluu

SOLUTIONS

1

Gluu ENTERPRISE

Gluu ENTERPRISE is a software subscription for self-hosting which includes the integration of various open source IAM components.

2

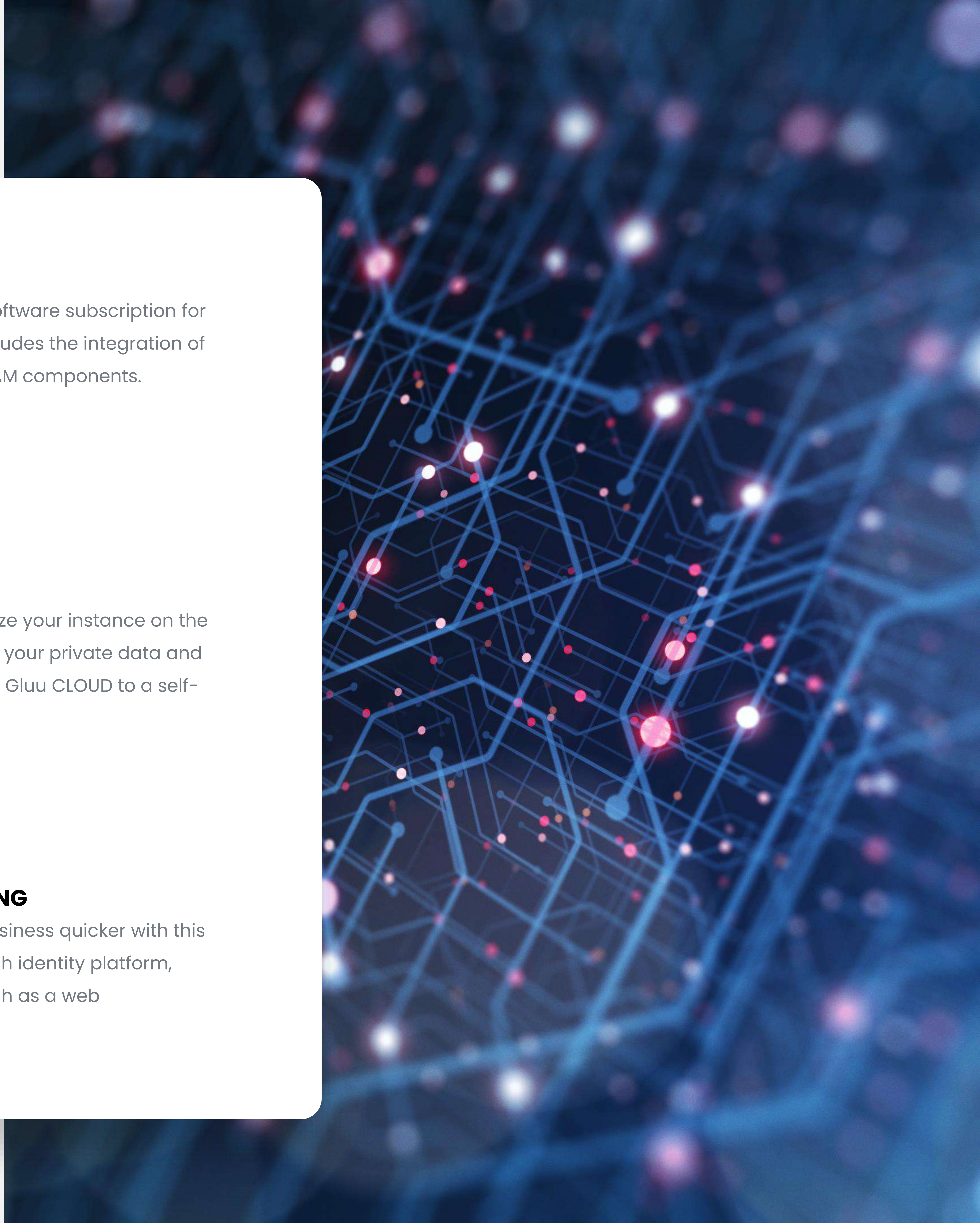
Gluu CLOUD

Fully own and customize your instance on the server or migrate both your private data and configuration from the Gluu CLOUD to a self-hosted Gluu Server.

3

Gluu OPEN BANKING

Open your bank for business quicker with this secure and feature-rich identity platform, including add-ons such as a web administration panel.



>

Want to be a product partner?

We partner with - and are always seeking - leading global brands with new innovations to bring emerging authentication technologies to the market. And as a truly value-added distributor, we focus on niche products to grow a strong market and fulfil that growth potential and trajectory.

In-house **SOLUTIONS**

We’ve designed a suite of security management systems that takes care of your authorization and encryption needs for a secure operational process.

Identity Management

Cross-network data restriction system for authorized personnel only.

Cloud Security

Framework of services to protect cloud-based data.

Strong Authentication

Layered authentication system for a more secure access.

Public Key Infrastructure

360-encryption and decryption solution for sensitive digital data.

Identity & Access **Management**

IAM is a 2-part authentication solution.

Identity management: confirms who you are

Access management: grants you the appropriate level of access.

Single Sign-On

One set of credentials for all access areas

Multi-Factor Authentication (MFA)

Multi-layered process for increased filtration and security

User lifecycle management

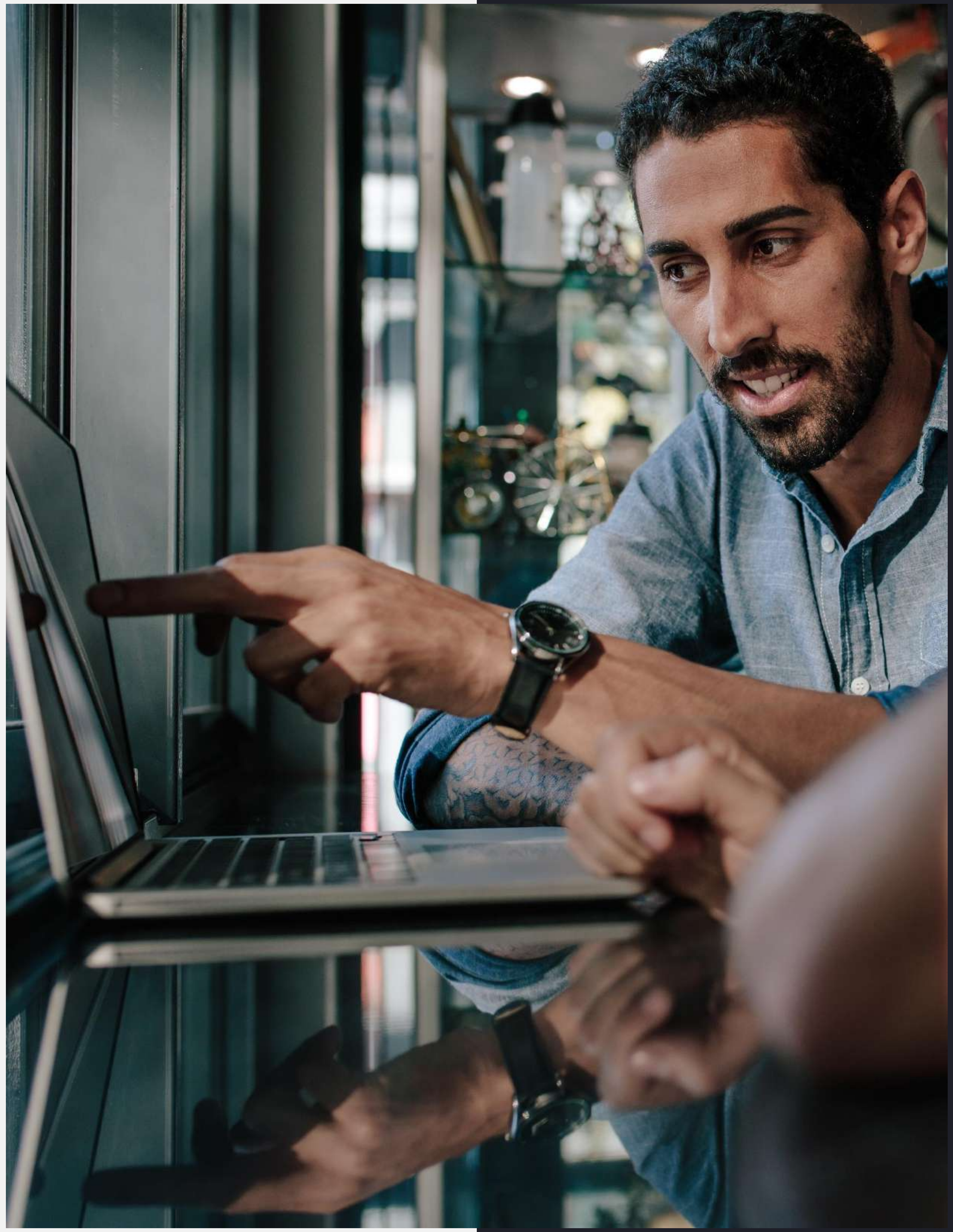
IAM tools to quickly appropriate access to users based on job functions.

Reporting

Easy generation of reports and logs to assess future risks as well as ensure compliance.

>

Why you need Identity & Access Management



Only authorized individuals have access to authorized data

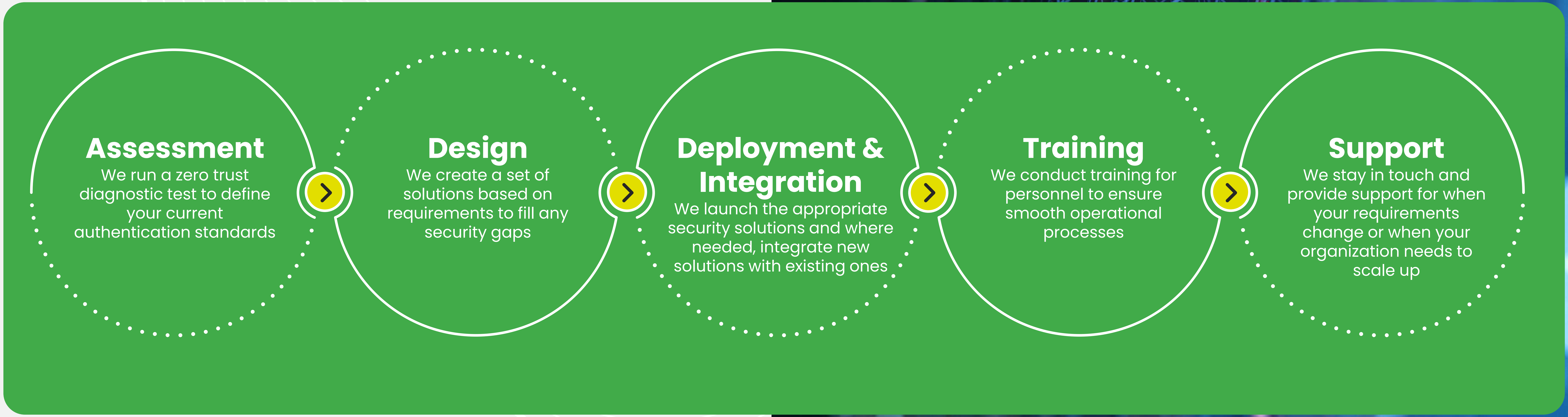
A stronger defence against data breaches

Better compliance with security standards regulations

Better productivity through automation

An environment for information sharing and greater collaboration.

Our approach to IAM



Assessment

We run a zero trust diagnostic test to define your current authentication standards

Design

We create a set of solutions based on requirements to fill any security gaps

Deployment & Integration

We launch the appropriate security solutions and where needed, integrate new solutions with existing ones

Training

We conduct training for personnel to ensure smooth operational processes

Support

We stay in touch and provide support for when your requirements change or when your organization needs to scale up

>

Cloud **Security**

Higher protection, increased flexibility

Cloud security is a framework of solutions to safeguard cloud-based data and infrastructure.

Authentication controls

Seek or prevent unauthorized access and automate privilege management.

Data encryption

Robust automatic data encryption both in transit and at rest.

Centralized visibility

Monitoring of security infrastructure such as user activity to assess security status.

Threat Management

Allows for quick proactive risk mitigation or implement reactionary measures.

Seamless integration

Integrate with existing security protocols to ensure a smooth operational process.

Why you need **Cloud Security**

Enterprise-level security via superior security infrastructure

Better scalability and quicker deployment time

Lower upfront costs

Consistent updates and patches

Efficient replication of data

Ease of integration

Our approach to IAM

Assessment

We review your existing security standard and capabilities, benchmarking it against regulatory standards and identify gaps.

Design

We create a roadmap for your organization’s cloud strategy based on objectives, risk mitigation and compliance. We also develop future-proof security strategies for a more proactive security approach.

Deployment

We launch the cloud-specific security protocols and integrate the system with existing security functions.

Transition

We progressively and methodically move your organization to the new cloud security system and onboard personnel until you’re fully migrated

Support

We stay in touch and provide information on updates and patches while also introducing new industry best practices

Strong **Authentication**

Impenetrable gatekeeping

Strong Authentication combines 2 or more methods of authenticating your identity.

These secondary security measures are generally divided into 3 factors:

Knowledge Factor
or something you know

Personal information that only the user knows such as passwords, PINs, security questions, etc.

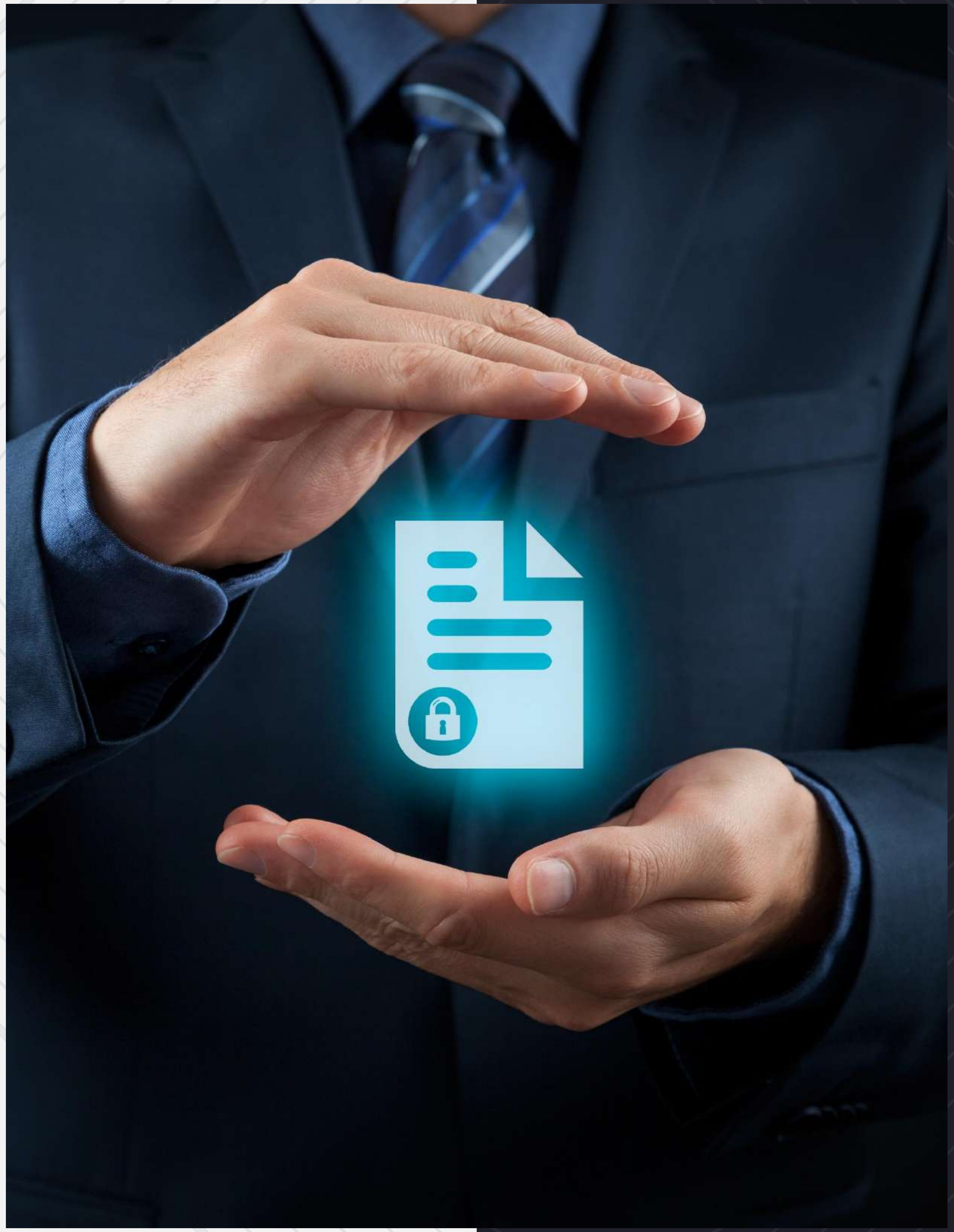
Possession Factor
or something you have

Hardware-based authentication method using cards, security keys or a one-time password (OTP)

Inherence Factor
or something you are

Something unique to the users including fingerprint- scanning or iris and face-recognition and other biometric systems.

Why you need Strong **Authentication**

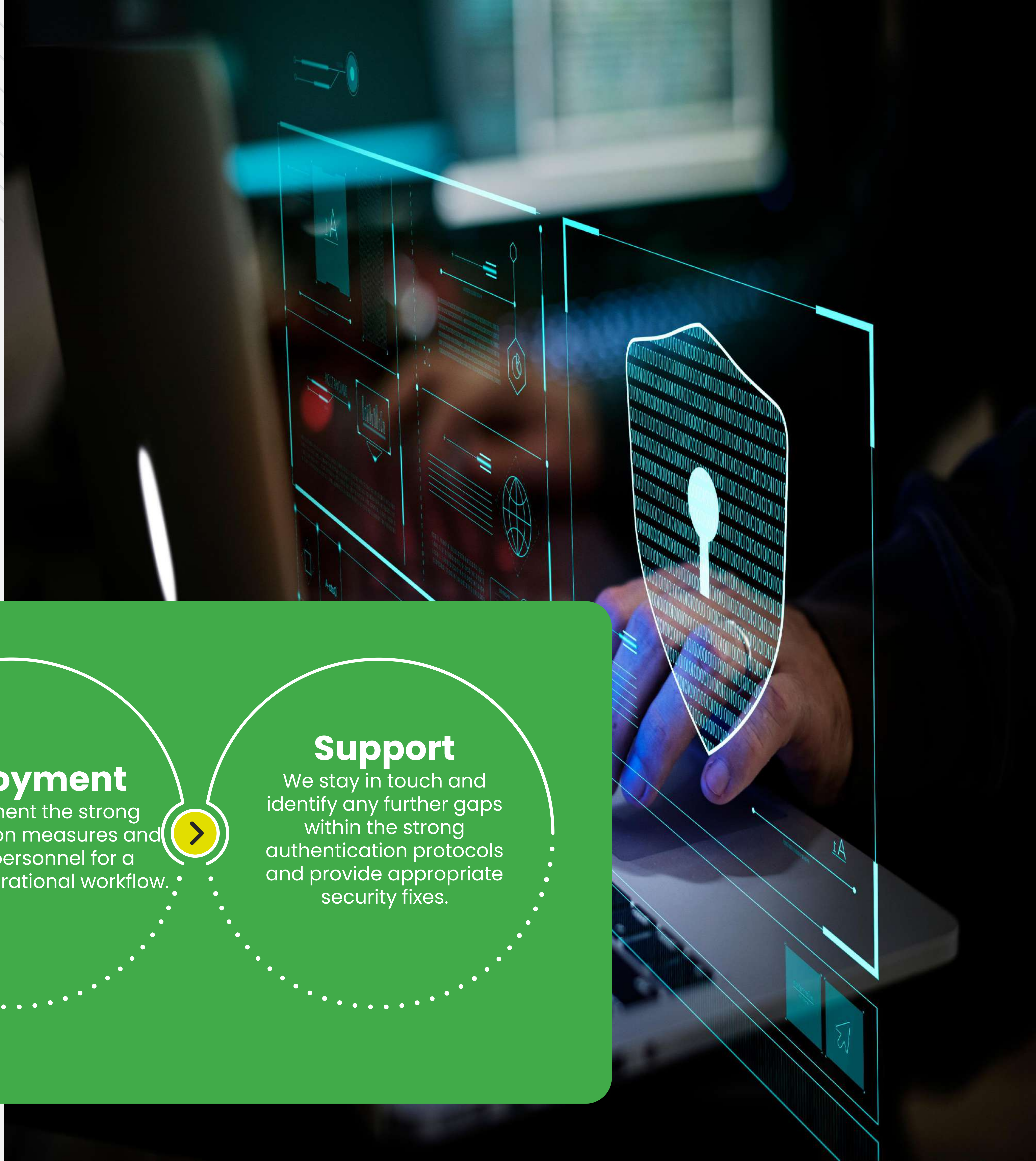


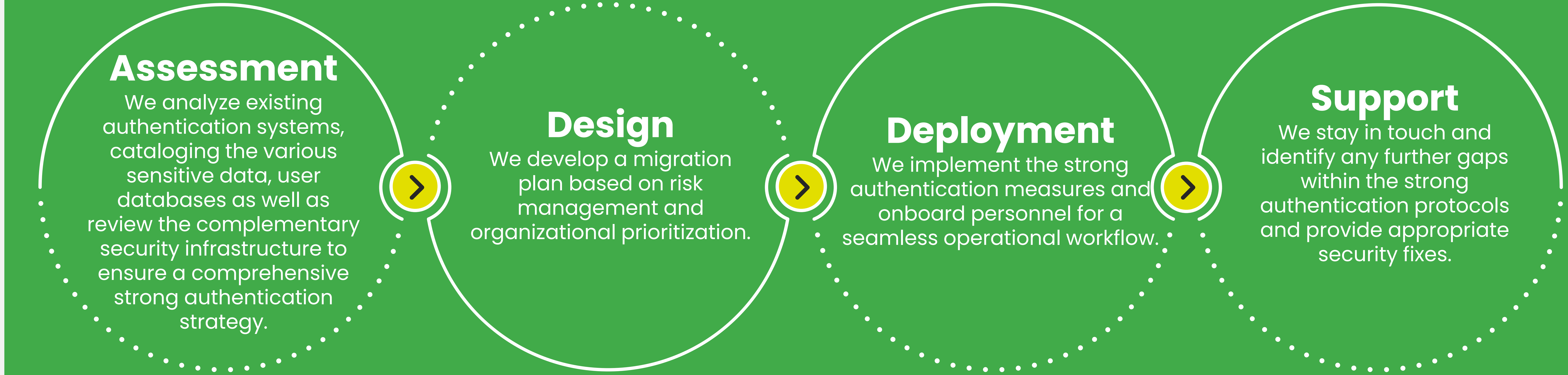
increased security for identity and access

reliable, high-success solution

regulatory compliance

Our approach to Strong Authentication





Assessment

We analyze existing authentication systems, cataloging the various sensitive data, user databases as well as review the complementary security infrastructure to ensure a comprehensive strong authentication strategy.

Design

We develop a migration plan based on risk management and organizational prioritization.

Deployment

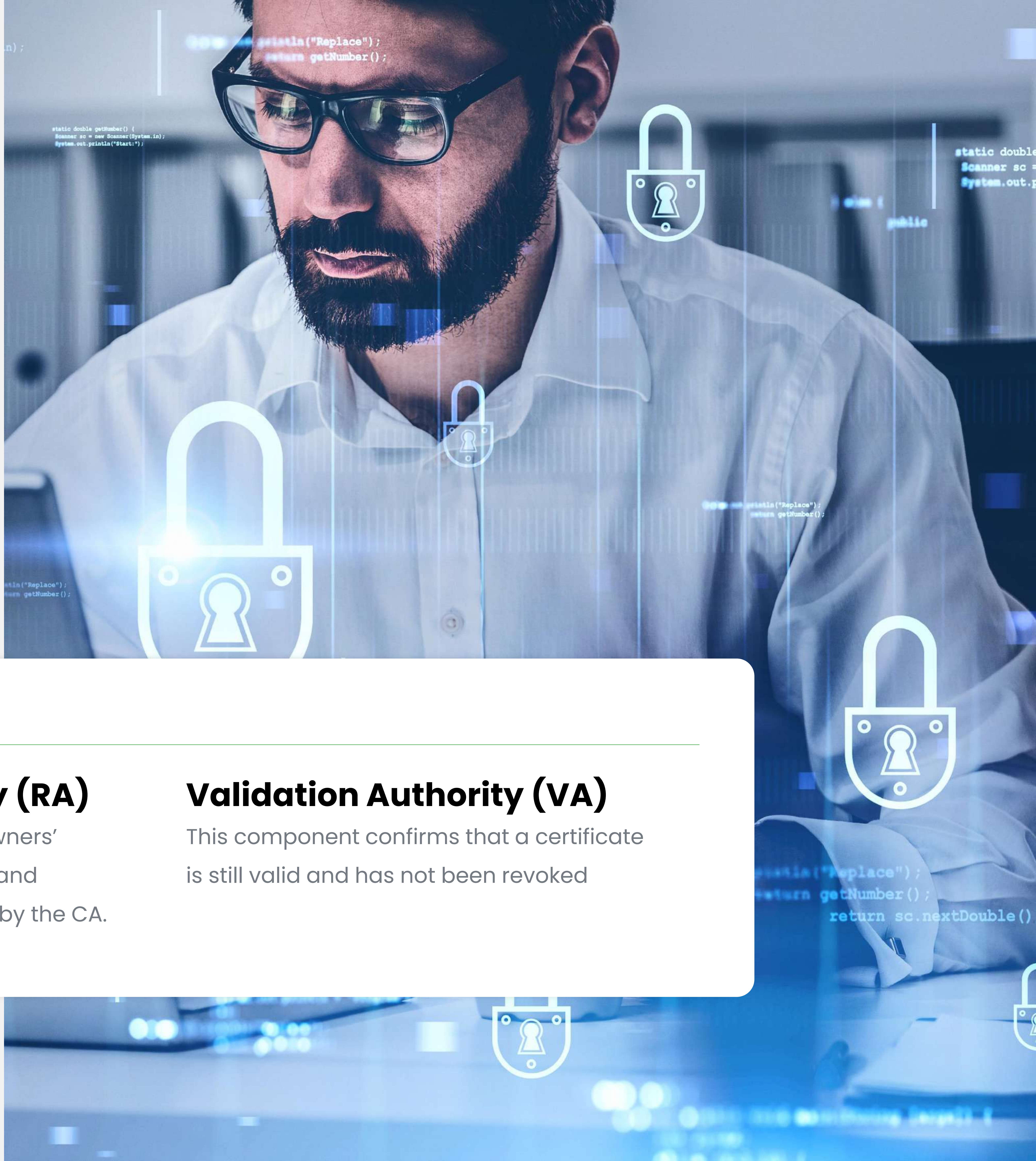
We implement the strong authentication measures and onboard personnel for a seamless operational workflow.

Support

We stay in touch and identify any further gaps within the strong authentication protocols and provide appropriate security fixes.

Public Key **Infrastructure**

Public Key Infrastructure (PKI) is the technology behind digital certificates, an encryption mechanism that relies upon the use of two keys - a public key and a private key - which, when paired, decrypts and transmits the original message.



A PKI implements 3 critical components

Certificate Authority (CA)

This component acts as the issuer and signee of the digital certificates, and is trusted by all other entities.

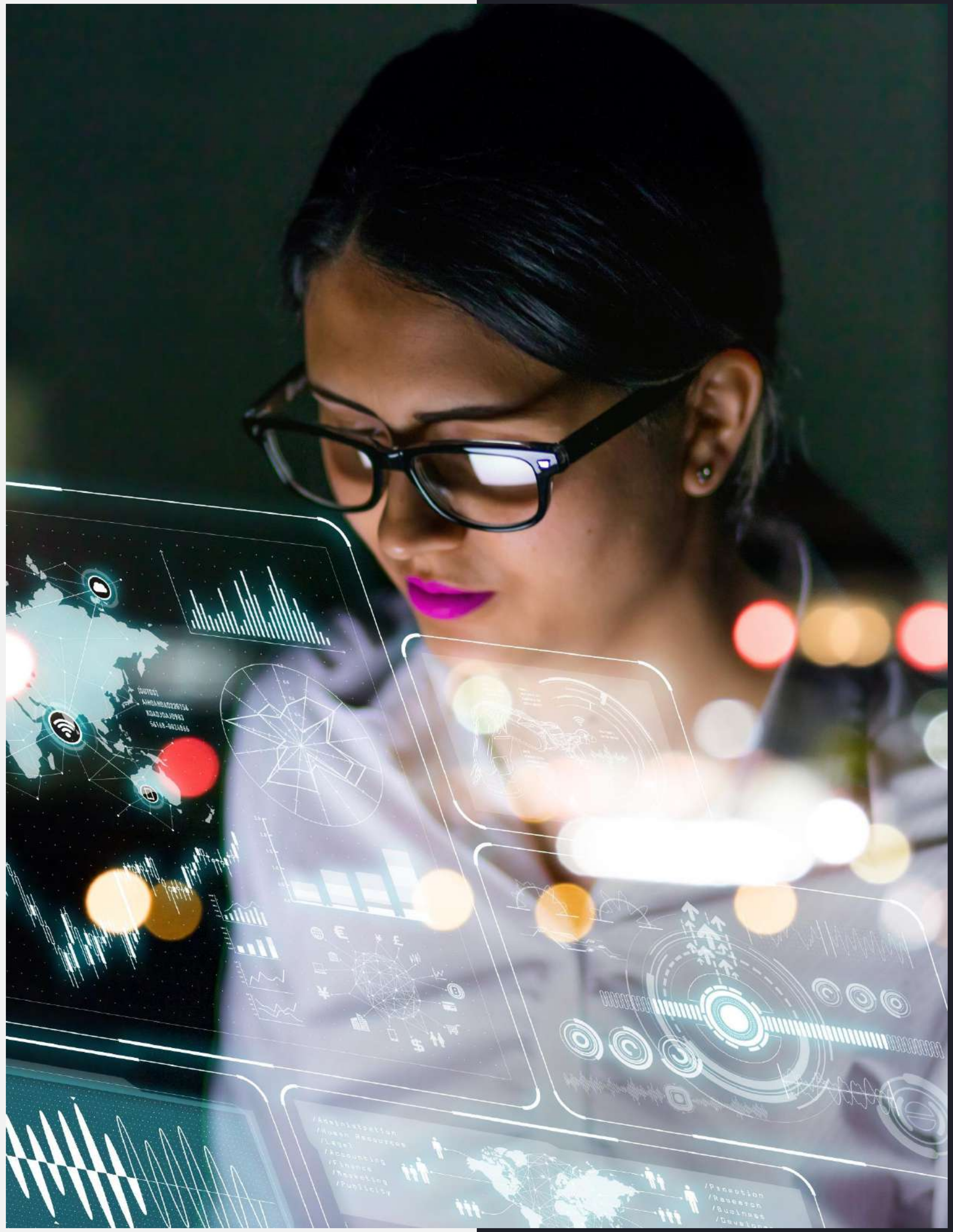
Registration Authority (RA)

This is where the identity of the owners' digital certificates are registered and cross-checked before it is issued by the CA.

Validation Authority (VA)

This component confirms that a certificate is still valid and has not been revoked

Why you need **Public Key Infrastructure**



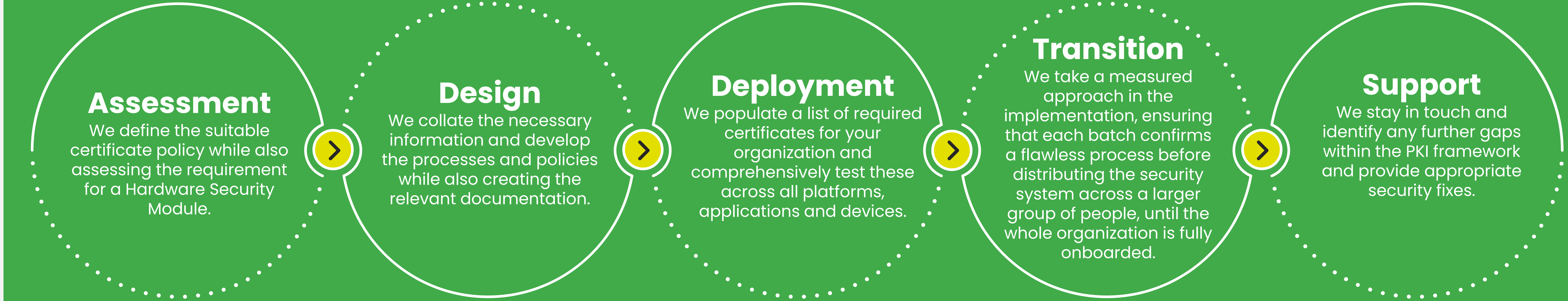
The establishment of trust, internally and externally

Smooth transfer of data

Correct authorization of individuals

Increased data and identity security at a large scale, with potential to be further scaled up

Our approach to IAM



Assessment
We define the suitable certificate policy while also assessing the requirement for a Hardware Security Module.

Design
We collate the necessary information and develop the processes and policies while also creating the relevant documentation.

Deployment
We populate a list of required certificates for your organization and comprehensively test these across all platforms, applications and devices.

Transition
We take a measured approach in the implementation, ensuring that each batch confirms a flawless process before distributing the security system across a larger group of people, until the whole organization is fully onboarded.

Support
We stay in touch and identify any further gaps within the PKI framework and provide appropriate security fixes.

We’ve been around.

Over 30 years.
Countless organizations protected.
More than 35,000 cyber attacks prevented.

>the_kernel / We don’t panic

The Kernel Headquarters
United Arab Emirates

Phone +971 4 7017 260 / 1 / 2

Email info@thekernel.com
P.O Box: 54808
2216 Churchill Tower, Business Bay, Dubai, UAE

Ukraine

Phone Tel: +38 (044) 506 1999

Email info@thekernel.ua
10, Hrushevskoho, office 212, 01001, Kiyv, Ukraine

Visit our website