WHITE PAPER

HYPR | The Cyber Hut

Toward Converged Identity Assurance

Table of Contents

Introduction

- The importance of IAM is increasing to support business and security use cases across B2E and B2C
- IAM core services manual and siloed while infrastructure is fragmented and under automated attacks
- Application of Identity Assurance across all parts of identity lifecycle improves security and productivity

Importance of IAM Increasing

Identity and Access Management has become a crucial component of both the Chief Information Security Officers (CISO) defensive arsenal and as a key business enabler for those leading digital transformation (DX) across the modern enterprise.

The rise over the past decade of Zero Trust network architecture (ZTNA) as the main approach to selecting and deploying network and data security controls has resulted in a more **foundational** need for **core IAM** technologies. These technologies are more closely integrated, composable and modular than previously deployed and provide business leaders with a more agile and adaptive approach to enterprise security that is flexible and measurable.

The productivity gains now achievable by the deployment of modern IAM technologies supports not only operational cost savings from the automation of key business processes, but also enables joint ventures, rapid launches of new products and improves competitive agility, by making sure the right users get access to the right data at the right time.

However, this modern opportunity has brought challenges and risks.

IAM Infrastructure Fragmentation

The implementation of IAM technologies over the past two decades has led to an often **fragmented** array of directories, single sign-on solutions, MFA components and access control capabilities — all hampered by **manual process** and **poor visibility.** The trust boundaries across this patch-work quilt of vendors and solutions has proved to be an ideal attack vector for automated adversarial activity, with poor detection and remediation capabilities allowing credential theft, privilege abuse and identity fraud and impersonation to proliferate.

Application of Identity Assurance

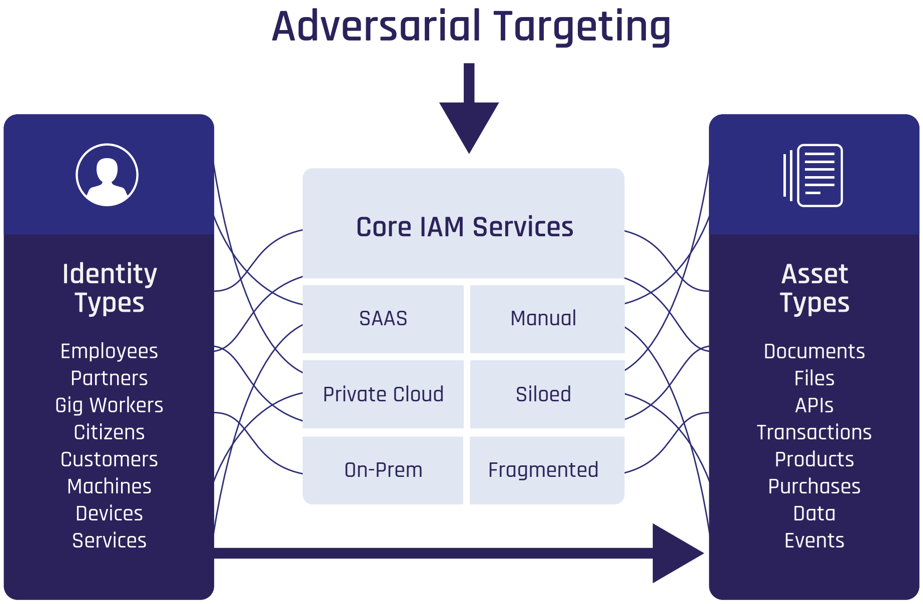
To that end, and as strong authentication has increased in both deployment coverage and maturity of solutions, the **convergence** of **identity assurance** capabilities into this segment has emerged as a key requirement. This results in improvements from both an identity controls and security perspective as well as increased productivity and operational efficiency. Such operational efficiency arises from more accurate and auditable ways to verify the employee identity information during *onboarding, credential reset* and *access request* workflows.

Enterprise Business Challenges

- Technology landscape increasing in complexity — with hybrid deployments, technology silos, poor visibility and metrics
- Manual and disconnected processes for employee onboarding and credential management
- Remote working and people supply chains increasing in volume and variety

Complex Technology Landscape

Due to the historical nature of core IAM service deployment, many organizations often face the **operational** and **security** burden of having to manage a fragmented landscape. This **fragmentation** has resulted in capabilities being **distributed,** with different owners and metrics, all having to serve an ever-increasing variety and volume of identity types and assets they need to access.



Manual & Disconnected Processes

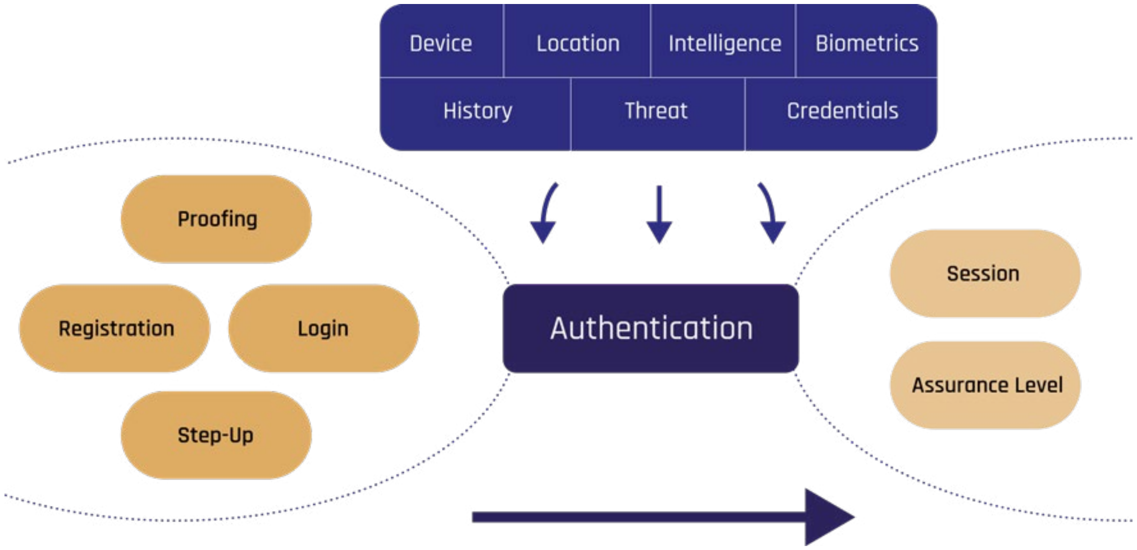
In this fragmented landscape, a main source of inconsistent policy application, errors and poor reporting is associated with the manual processes that still exist for the **employee onboarding, credential issuance, and credential re-issuance** workflows. These workflows are crucial for both employee productivity and corporate security — yet are often fulfilled via disconnected ticketing. Not only does this introduce productivity concerns, this disconnected model provides an ideal opportunity for adversarial activity — activity that is often becoming highly automated and difficult to monitor and identify.

Remote Working & Distributed Corporate Operations

To amplify the weaknesses often associated with manual onboarding, many organizations now have to support an ever-increasing number of employees working from home and **remote office** locations. It is not uncommon for employees to be entirely on-boarded without entering a corporate office — with equipment, login accounts and credentials all provisioned remotely without ever meeting in person. The reliance on partner organizations, suppliers and joint ventures to deliver services increases the **volume** and **variety** of **employee** and **contractor** management tasks. This increases risk exposure and introduces employee productivity friction.

Enterprise Authentication Challenges

- Authentication as pinch point for user interactions — provides opportunities and challenges
- Organizations have multiple MFA solutions — but no pathway to consolidation, a unified experience and passwordless
- Identity verification and validation isolated and not-continuous



Authentication (that is FIDO based and phishing resistant) is a key aspect of application and service access — providing an opportunity for **security control** and user **interaction.** Today's modern enterprise has to support a broad array of applications, services and desktop-to-cloud journeys, which require authentication capabilities to not only be **consistent** across these applications and user groups but also provide **integration options** that can help support consolidation and migration (from legacy MFA and password-based options).

Historically the identity proofing and verification capabilities have been separate from the authentication function, resulting in siloed deployments, artificial trust boundaries and opportunities for compromise. This manual hand off from the employee onboarding process into the credential issuance and authentication steps is inefficient and insecure.

Business Impact

- Cumbersome and ineffective employee verification leading to employee fraud
- Credential theft and account takeover leading to data breaches
- A lack of post-login ongoing security contributing to session and access control risk

Cumbersome and ineffective employee validation and verification functions are leading to increased numbers of **employee fraud** — where the link between employee onboarding, credential and equipment issuance and day to day authentication and work interactions are disconnected and manual.

In mid to large enterprises, where staff often join and onboard from remote locations, a **lack** of **joined** up **processes** and workflow for the identity validation and verification process is contributing to risk of employee performance fraud — where the employee who is interviewed is not the same person performing day to day tasks.

In addition, sophisticated (yet often highly automated) cyberattacks are relying on siloed authentication services that do not contain sufficiently strong nor phishing-resistant capabilities, to establish credential access via credential interception, phishing and ultimate theft and re-use.

Emergence of Converged Identity Assurance

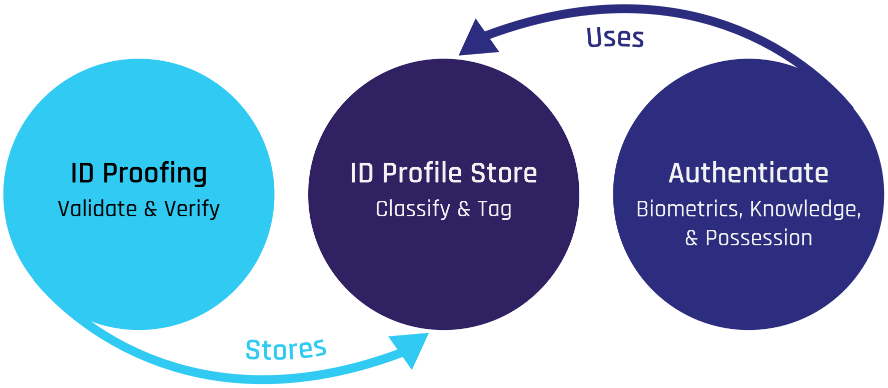
- View authentication in stages of maturity — from being siloed and coarse grained to being reliant on an assured identity that is continually verified
- Look to reduce fragmentation and trust boundaries
- Overlay existing authentication with verified identities — continually

Authentication is a **journey** and organizations of all sizes will be at different stages in their maturity — from leveraging single factor authentication with coarse grained analysis and responses, through to the emergence of identity assurance capabilities that are seamlessly integrated into the authentication and credentials lifecycle.

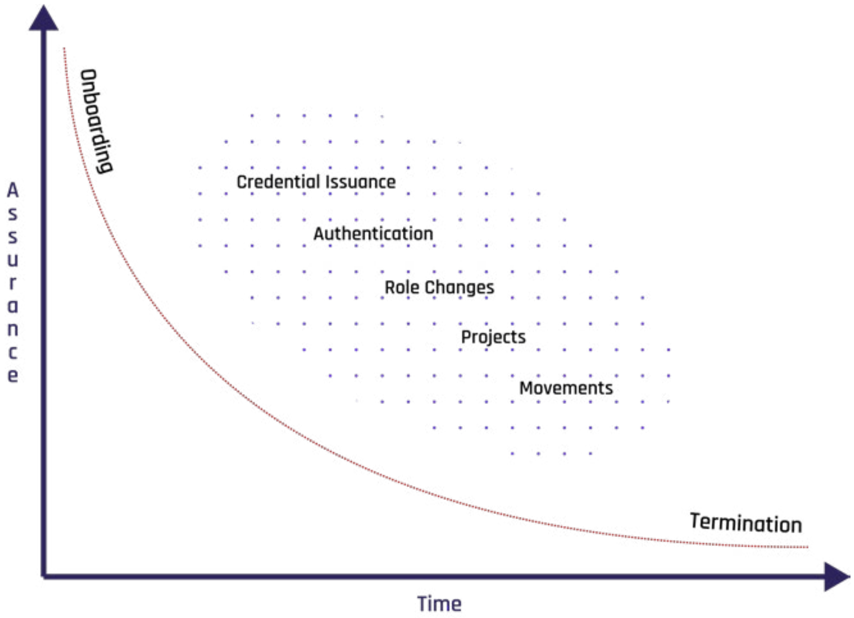
The classic basic building blocks of authentication can be described in four stages, where a service is starting from a position of limited information that cannot be triangulated with more trusted sources of assurance, through to the monitoring of identity assurance and authentication assurance data during usage.

Firstly, these stages need to be well **integrated, modular** with **fine grained** decision points that can allow for the integration of different data sources (including and especially non-identity data signals) as well as the ability to continually reverify data at each stage of the process. Responses to change (or the identification of higher levels of risk) need to be both adaptive (change as the context changes) and fine grained — meaning that small changes can be implemented.

A typical enterprise authentication solution, even if leveraging features such a MFA, will often be grounded by self-asserted identity data, or be disconnected from any identity proofing and verification functions that have taken place during identity onboarding.



The traditionally separate identity verification and proofing service is often only triggered once during employee onboarding — not throughout the identity lifecycle. The onboarding process is also likely to be constrained by having to be physical in nature, tied to particular document analysis options and perhaps only for the most high-risk job roles too.

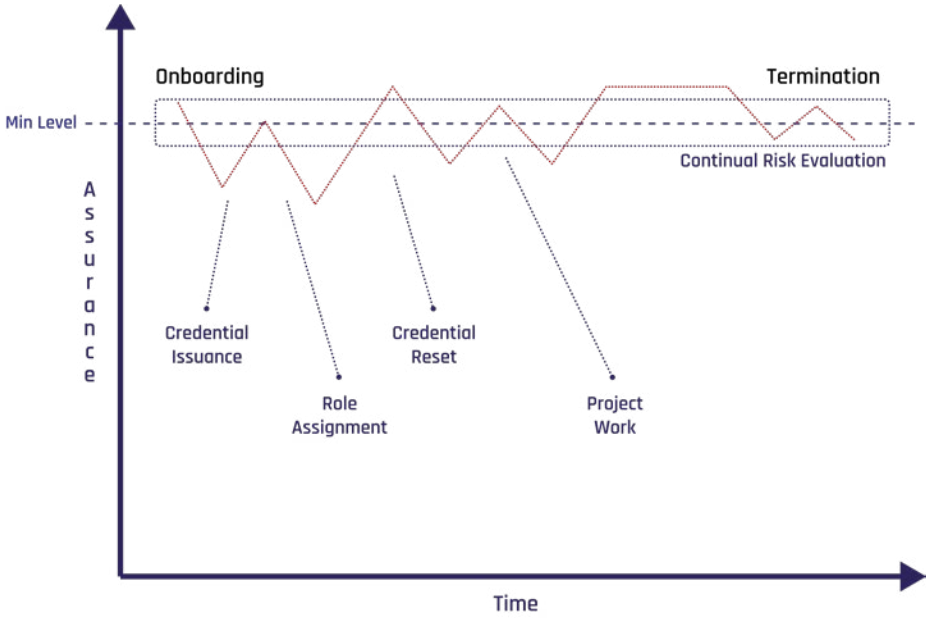


The identity lifecycle however will undergo both persistent **data changes** and **runtime behaviors** that are not tied back to the assured identity. This lifecycle will include credential issuance and reset flows, authentication, role assignments, project work or more contextually specific events.

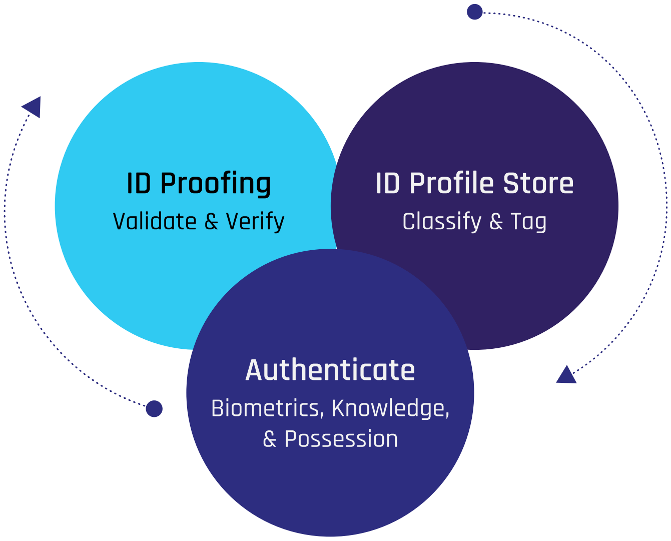
To that end, a more consistent and stable approach to identity assurance is required, that helps firstly remove the downward degradation associated with more isolated approaches, and second applies continual risk analysis to every stage of the identity and credential lifecycles.

This helps to firstly identify risk associated with individual identity events, but secondly allow that risk to be treated in a way that allows it to be consistently within known thresholds.

Identity risk in turn, ends up being more continually managed, with re-verification, validation and authentication becoming seamlessly integrated into a range of events — from credential reset, job function change and more.



A more **risk focused and converged** approach to identity assurance, will see continual evaluation of an identity lifecycle event (through non-identity signals analysis) as well being able to apply fine grained responses, that are not only linked back to the identity assurance function, but leverage that assurance data to reduce risk and keep the identity assurance level within range of known risk thresholds. The continual analysis of identity and non-identity data throughout the identity event lifecycle provides a more rounded and converged approach to assurance.



Continual Risk Analysis & Treatment

The requirement of integrating identity assurance to **all parts of the identity lifecycle** requires different signals to analyze as well as the automation of different end user interactions. Signals analysis will likely leverage non-identity data points such as the user device and its characteristics and risk posture, the current location, transaction details and peer group comparison.

End user interactions throughout the identity lifecycle will require instant messaging, video, chat and document verification functions — functions that would historically have been performed physically, but now need to be **performed digitally.**

Capability Analysis

What capabilities should be included in a converged identity assurance approach?

Identity Verification & Validation

AREA	CAPABILITY
Sources	● Ability to integrate document-based verification functions (e.g., driving license, passport, employee IDs) ● Ability to integrate video-based verification functions ● Ability to integrate face recognition functions ● Ability to integrate chat base verification functions ● Ability to identify and integrate manager approval during verification functions ● Ability to detect deep fakes and other activities that attempt to trick the verification process to issue false positives or negatives
Lifecycle Coverage	● Ability to remotely collect identity evidence ● Ability to support verification functions to permanent employees ● Ability to support verification functions to contract staff ● Ability to support verification functions to partner staff ● Ability to support verification functions during identity onboarding ● Ability to support verification functions during identity job change ● Ability to support verification functions by event triggering (credential reset, high risk translation)
Integration	● Ability to have a policy-based verification function (which is adaptable based on unique requirements) ● Leverage signals from the full security ecosystem ● Ability to support different identity types at different parts of their lifecycle

Contextual & Adaptive Risk Analysis

AREA	CAPABILITY
Sources	● Ability to analyze a range of non-identity signals ● Ability to analyze device characteristics (versions, software, hardware, jailbreak detection) ● Ability to analyze location characteristics (IP, co-ords) ● Ability to analyze browser characteristics ● Ability to analyze individual transaction information ● Ability to analyze individual historical transaction information ● Ability to analyze individual historical behavioral information ● Ability to analyze individual against peers ● Ability to define peer groups
Lifecycle Coverage	● Ability to analyze signals throughout the identity lifecycle ● Ability to analyze risk during identity onboarding ● Ability to analyze risk during authentication ● Ability to analyze risk during session ● Ability to analyze risk during access control / authorization requests ● Ability to analyze risk during password reset ● Ability to analyze risk during credential lifecycle (issuance, reset, use, reset, and removal)
Integration	● Ability to share risk analysis with a variety of targets ● Ability to share risk analysis information with SOAR tools ● Ability to share risk analysis information with SIEM tools ● Ability to share risk analysis information with post login events (access control) ● Ability to query risk analysis information via an API

Strong Authentication

AREA	CAPABILITY
Sources	● Ability to support phishing resistant authentication ● Ability to support cryptographic challenge response authentication ● Ability to support possession-based authentication via ownership of private key in secure mobile storage ● Ability to support local native biometric authentication via mobile fingerprint / facial ID ● Ability to issue credentials without a shared secret ● Ability to provide authentication services with or without an app ● Ability to support existing and emerging authentication standards such as FIDO/FIDO2/WebAuthn/CTAP, NIST 800-63, PSD2/SCA
Lifecycle Coverage	● Ability to provide consistent authentication services to different identity types (consumers, employees, partners, contractors) ● Ability to provide authentication services to high-risk events such as privileged access, consumer online transactions ● Ability to provide authentication services to physical components (doors) ● Ability to provide authentication services for transaction signing ● Ability to authenticate addition of secondary device / device migration ● Ability to reset/revoke previously issued credentials
Integration	● Ability to integrate authentication services to existing identity provider infrastructure ● Ability to integrate authentication services via an API ● Ability to integrate authentication services via a QR code ● Ability to integrate consistent authentication services across different devices ● Ability to integrate consistent authentication services across downstream applications ● Ability to have a single console for authentication service management ● Ability to provide consistent authentication services during Windows desktop login ● Ability to provide consistent authentication services from desktop to cloud ● Ability to provide migration strategies from existing MFA solutions ● Ability to provide migration strategies from existing shared secret / password-based authentication solutions

Benefits

Improved Identity Security

An ability to improve identity security across the entire organization, entire identity lifecycle and across the entire application landscape. Provides a migration to support NIST 800-63b **Authentication Assurance Level (AAL) level 2 and 3** — cryptographic, phishing resistant challenge response authentication with identity verification to reduce impersonation and account takeover.

Accelerated Adoption of Zero Trust

Zero trust, and its approach of "trust but verify" requires a need for not only strong authentication, but also the ability to leverage strong authentication across a range of different resources — from desktop to the cloud — all within a remotely deployed environment where the identity and device are in uncontrolled environments. The ability to bind an authentication event to a verified identity supports this secure architecture.

Accelerated Password Migration

A broad array of integration options, coupled with a more converged assurance and authentication landscape, provides a foundation for the migration of passwords and shared secret style authentication modals. Consolidation of passwordless login via a broad and simple integration model helps deliver a consistent end-to-end verification experience.

Improved IAM Productivity

Converged approaches to verification and authentication reduce the agent assisted workload, by providing an array of secure self-service options for credential reset, credential issuance, onboarding and access request flows.

Reduced Compliance Exposure

Who has access to what is still a complex process to deliver. By automating the identity verification, authentication and authorization functions, improved visibility and operational management is achieved allowing accounts to be tied to real, securely verified physical identities.

Example User Stories

AS A…	I WANT TO…	SO I CAN…	CONTEXT
As an application owner	I want to link access to a real identity	so I can improve compliance visibility	End to end identity verification to provide context to compliance reporting
As a CIO	I want to remove identity siloes associated with verification	so I can improve operational efficiencies	Reduce identity tooling and provide improved identity risk and data integration
As a CISO	I want to deliver secure remote onboarding	so I can improve employee productivity and security	Remote onboarding is a key enabler to business productivity
As a compliance manager	I want to bind authentication events to verified physical identities	so I can confidently answer (via automation) "who has access to what" post authentication	Reduction of isolation between identity proofing, authentication and access
As HR	I want to integrate the employee on boarding process with login events	so I can reduce the incidence of employee fraud that occurs between onboarding and job function execution	Reducing risking across employee lifecycle
As an identity architect	I want to have a consistent way of authenticating staff	so I can reduce the MFA attack surface with modern phishing resistant approaches	Migration from passwords and legacy MFA to a consistent platform reduces risk
As a line of business manager	I want to leverage instant message for IAM approvals	so I can reduce the need for siloed tooling	Allowing verification to take place at all parts of the IAM lifecycle provides the right people with the right information at the right time

Recommendations

A converged approach to identity assurance provides productivity, security and business enablement improvements. Today's complex, manual and fragmented approach to identity assurance can be improved by a more integrated and continual approach to verification and validation, supporting risk analysis and fine-grained responses to many aspects of the identity onboarding, authentication and access control functions.

Organizations can get started on this journey by:

- Understanding their existing identity onboarding processes
- Creating an inventory of existing authentication components — along with their security and usability capabilities
- Performing threat modeling and attack path analysis of identity lifecycle journeys
- Identifying high-risk applications and phases for migration

About The Cyber Hut

The Cyber Hut is a leading boutique industry analyst and advisory firm based out of the UK. The Cyber Hut is home to the IAM2 Industry Analysis Map that continually tracks over 50 IAM vendors, the IAM Radar, a curated headlines and commentary resource, The Week in Identity Podcast and a range of research, advisory, training, assessment and inquiry services. For more information, visit www.thecyberhut.com.

See how HYPR Identity Assurance can secure your workforce and customers

Visit hypr.com/get-a-demo

HYPR

About HYPR

HYPR creates trust in the identity lifecycle. HYPR Identity Assurance provides the strongest end-to-end identity security for your workforce and customers, combining modern passwordless authentication with adaptive risk mitigation, automated identity verification and a simple, intuitive user experience. HYPR protects your users, services and brand reputation now, with the flexibility and forward compatibility to meet future evolving conditions. HYPR has a demonstrated track record securing organizations globally, with deployments in some of the most complex and demanding environments, including 2 of the 4 largest US banks, leading critical infrastructure companies and other technology-forward businesses. HYPR's solutions have been independently validated to return a 324% ROI.