




## Converged Identity Assurance:

# Capability Analysis

Experts increasingly recommend that organizations implement a holistic Identity Assurance approach to address today's many IAM business and security challenges. This document lists key capabilities organizations should consider when building a converged identity assurance approach.




## Identity Verification & Validation

In today's connected world, identity verification cannot stop at onboarding. It should be integrated and continual, leveraging multiple identity proofing and verification technologies.

AREA	CAPABILITY
 <p><b>Sources</b></p>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Ability to integrate document-based verification functions (e.g., driving license, passport, employee IDs)</li> <li><input type="checkbox"/> Ability to integrate video-based verification functions</li> <li><input type="checkbox"/> Ability to integrate face recognition functions</li> <li><input type="checkbox"/> Ability to integrate chat base verification functions</li> <li><input type="checkbox"/> Ability to identify and integrate manager approval during verification functions</li> <li><input type="checkbox"/> Ability to detect deep fakes and other activities that attempt to trick the verification process to issue false positives or negatives</li> </ul>
 <p><b>Lifecycle Coverage</b></p>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Ability to remotely collect identity evidence</li> <li><input type="checkbox"/> Ability to support verification functions to permanent employees</li> <li><input type="checkbox"/> Ability to support verification functions to contract staff</li> <li><input type="checkbox"/> Ability to support verification functions to partner staff</li> <li><input type="checkbox"/> Ability to support verification functions during identity onboarding</li> <li><input type="checkbox"/> Ability to support verification functions during identity job change</li> <li><input type="checkbox"/> Ability to support verification functions by event triggering (credential reset, high risk translation)</li> </ul>
 <p><b>Integration</b></p>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Ability to have a policy-based verification function (which is adaptable based on unique requirements)</li> <li><input type="checkbox"/> Leverage signals from the full security ecosystem</li> <li><input type="checkbox"/> Ability to support different identity types at different parts of their lifecycle</li> </ul>

## Strong Authentication

Phishing-resistant, FIDO-based authentication is a key aspect of application and service access. Today’s modern enterprise has to support a broad array of applications, services and desktop-to-cloud journeys.

AREA	CAPABILITY
 <p><b>Sources</b></p>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Ability to support phishing resistant authentication</li> <li><input type="checkbox"/> Ability to support cryptographic challenge response authentication</li> <li><input type="checkbox"/> Ability to support possession-based authentication via ownership of private key in secure mobile storage</li> <li><input type="checkbox"/> Ability to support local native biometric authentication via mobile fingerprint / facial ID</li> <li><input type="checkbox"/> Ability to issue credentials without a shared secret</li> <li><input type="checkbox"/> Ability to provide authentication services with or without an app</li> <li><input type="checkbox"/> Ability to support existing and emerging authentication standards such as FIDO/ FIDO2/WebAuthn/CTAP, NIST 800-63, PSD2/SCA</li> </ul>
 <p><b>Lifecycle Coverage</b></p>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Ability to provide consistent authentication services to different identity types (consumers, employees, partners, contractors)</li> <li><input type="checkbox"/> Ability to provide authentication services to high-risk events such as privileged access, consumer online transactions</li> <li><input type="checkbox"/> Ability to provide authentication services to physical components (doors)</li> <li><input type="checkbox"/> Ability to provide authentication services for transaction signing</li> <li><input type="checkbox"/> Ability to authenticate addition of secondary device / device migration</li> <li><input type="checkbox"/> Ability to reset/revoke previously issued credentials</li> </ul>
 <p><b>Integration</b></p>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Ability to integrate authentication services to existing identity provider infrastructure</li> <li><input type="checkbox"/> Ability to integrate authentication services via an API</li> <li><input type="checkbox"/> Ability to integrate authentication services via a QR code</li> <li><input type="checkbox"/> Ability to integrate consistent authentication services across different devices</li> <li><input type="checkbox"/> Ability to integrate consistent authentication services across downstream applications</li> <li><input type="checkbox"/> Ability to have a single console for authentication service management</li> <li><input type="checkbox"/> Ability to provide consistent authentication services during Windows desktop login</li> <li><input type="checkbox"/> Ability to provide consistent authentication services from desktop to cloud</li> <li><input type="checkbox"/> Ability to provide migration strategies from existing MFA solutions</li> <li><input type="checkbox"/> Ability to provide migration strategies from existing shared secret / password-based authentication solutions</li> </ul>

## Contextual & Adaptive Risk Analysis

Comprehensive identity assurance requires integrated risk analysis based on multiple data sources and the ability to apply fine-grained, adaptive responses to all parts of the identity lifecycle.

AREA	CAPABILITY
 <p><b>Sources</b></p>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Ability to analyze a range of non-identity signals</li> <li><input type="checkbox"/> Ability to analyze device characteristics (versions, software, hardware, jailbreak detection)</li> <li><input type="checkbox"/> Ability to analyze location characteristics (IP, co-ords)</li> <li><input type="checkbox"/> Ability to analyze browser characteristics</li> <li><input type="checkbox"/> Ability to analyze individual transaction information</li> <li><input type="checkbox"/> Ability to analyze individual historical transaction information</li> <li><input type="checkbox"/> Ability to analyze individual historical behavioral information</li> <li><input type="checkbox"/> Ability to analyze individual against peers</li> <li><input type="checkbox"/> Ability to define peer groups</li> </ul>
 <p><b>Lifecycle Coverage</b></p>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Ability to analyze signals throughout the identity lifecycle</li> <li><input type="checkbox"/> Ability to analyze risk during identity onboarding</li> <li><input type="checkbox"/> Ability to analyze risk during authentication</li> <li><input type="checkbox"/> Ability to analyze risk during session</li> <li><input type="checkbox"/> Ability to analyze risk during access control / authorization requests</li> <li><input type="checkbox"/> Ability to analyze risk during password reset</li> <li><input type="checkbox"/> Ability to analyze risk during credential lifecycle (issuance, reset, use, reset, and removal)</li> </ul>
 <p><b>Integration</b></p>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Ability to share risk analysis with a variety of targets</li> <li><input type="checkbox"/> Ability to share risk analysis information with SOAR tools</li> <li><input type="checkbox"/> Ability to share risk analysis information with SIEM tools</li> <li><input type="checkbox"/> Ability to share risk analysis information with post login events (access control)</li> <li><input type="checkbox"/> Ability to query risk analysis information via an API</li> </ul>

## Learn how HYPR Identity Assurance can secure your workforce and customers

HYPR provides the strongest end-to-end identity security, combining phishing-resistant passwordless authentication with adaptive risk mitigation, automated identity verification and a simple, intuitive user experience.

FIND OUT MORE:

[hypr.com/contact](https://hypr.com/contact)