SOLUTION BRIEF

Stop AI Attacks With HYPR Identity Assurance

Prevent AI-assisted identity attacks through a comprehensive approach that leverages modern deterministic security controls and real-time identity risk mitigation

The proliferation of easily accessed AI tools is allowing cybercriminals to bypass traditional identity security controls at an unprecedented pace. Deepfakes, phishing, and social engineering attacks have all received a turbo boost as hackers find ever new creative ways to apply AI technologies. To combat this evolving risk landscape, organizations must adopt an identity security strategy that eliminates uncertainty yet can dynamically adapt to shifting conditions.

HYPR Identity Assurance takes a deterministic approach to securing identities while leveraging real-time risk intelligence to drive adaptive mitigation. By implementing these modern controls, organizations can significantly reduce their risk of identity fraud for both their workforce as well as customers.

Common AI-Assisted Attacks

Hackers use out of the box as well as specifically trained large language models (LLMs) to execute cyberattacks with frightening accuracy.

Phishing
In the post-AI era, hackers can use LLMs to tailor just about every phishing message to a specific target. They are in the local language, contain local context, and are largely indistinguishable from legitimate messages that people receive every day. A recent report found a 1,265% rise in phishing in 2023, largely due to the usage of AI tools.[1]

Impersonation (Deepfakes)
Identity theft is skyrocketing due to the ability of AI to impersonate an individual across all communication channels including voice, text and video. Hackers create convincing personas in minutes using samples of an individual's writing, publicly available videos and social media posts. A few years ago, creating a deepfake video required significant resources. Today, freely available apps can generate fairly accurate fakes, and they continue to improve daily.

Social Engineering
Before AI, social engineering attacks were highly manual with often low success rates. By using AI, hackers can mimic the tone, cadence, and contextual nuances of a specific target audience to achieve maximum yields. LLMs also are able to use reinforcement learning to improve with every conversation. These optimized algorithms can then be used to target large numbers of users simultaneously.

HYPR Key Benefits

- Prevent credential phishing and fraud with phishing-resistant MFA based on the FIDO passkey standards
- Stop identity impersonation and deepfake attacks with integrated, automated and comprehensive identity verification
- Combat identity fraud and risk through real-time identity risk analysis and mitigation
- Integrate quickly with existing systems, IdPs and applications
- Deploy a mature, enterprise proven solution that delivers validated ROI of 324%

[1] The State of Phishing 2023, SlashNext, October 2023

Why AI-Assisted Attacks Are So Successful

AI has become a major part of the attacker's toolkit for several reasons.

Speed and Scalability

AI can process and analyze data and conversations at speeds that outpace any human by orders of magnitude. This enables these tools to launch widespread attacks in a very short amount of time.

Adaptability

AI systems can quickly adapt their strategies based on a target's defense response. As a result, defense systems that rely on blocking known attack patterns are trivial for AI-assisted cyber tools to bypass.

Efficiency in Targeting

AI can analyze data from various sources to identify the most valuable targets. When AI identifies a series of patterns or signals, it can quickly train itself to focus on targets with the most likelihood for success. Most importantly, it can correlate with other AI systems that "soften the target," allowing it to more easily outflank an organizations' security controls. For example, one AI tool can launch a DDOS attack and, when the victim is in the midst of responding, another tool executes a highly contextualized phishing campaign that references the DDOS attack.

Leveraging Big Data

AI systems are able to integrate with countless public and private data sources, allowing attackers to refine strategies within minutes or seconds based on real-time events. Social media, breach data available on the dark web, and leaked credentials can all be processed instantaneously to create attacks with maximum impact.

The Failure of Probabilistic Identity Security Controls

The vast majority of identity security controls today are failing. Their probabilistic nature leaves major gaps that attackers can exploit using AI.

Phishable Authentication Factors

Passwords, one time passwords (OTP) delivered via SMS or app, and push notifications are the most common authentication methods in use today. AI can predict passwords with high accuracy, making brute force attacks trivial. It also strengthens phishing and social engineering to trick users into providing OTP codes or accepting push notifications. These methods are probabilistic as they cannot determine with certainty that the entity seeking access is the legitimate credential holder, and can be intercepted, replayed and phished.

KBA Identity Verification

AI systems can quickly ingest massive amounts of data about their targets to answer personal questions in real time, easily countering knowledge-based security methods. Combined with phishing and social engineering capabilities, AI-assisted hackers can quickly execute identity theft and gain access to employee and customer accounts.

Human-Verified Documents

To reduce identity fraud, many businesses have moved from KBA to online or in-person document verification. However, attackers can use widely available AI tools to create fake documents, including passports and driver licenses, that are able to fool many systems. Both human and machine-based verification controls of documents are probabilistic in nature as they can only determine the likelihood that a document is legitimate.

HYPR Defeats AI-Assisted Identity Attacks

HYPR allows you to be certain that a person is who they say they are at all times. Our Identity Assurance platform unites strong passwordless authentication, continuous risk mitigation and comprehensive identity verification to prevent automation and scaling of identity-related attacks.

Deterministic Security Controls

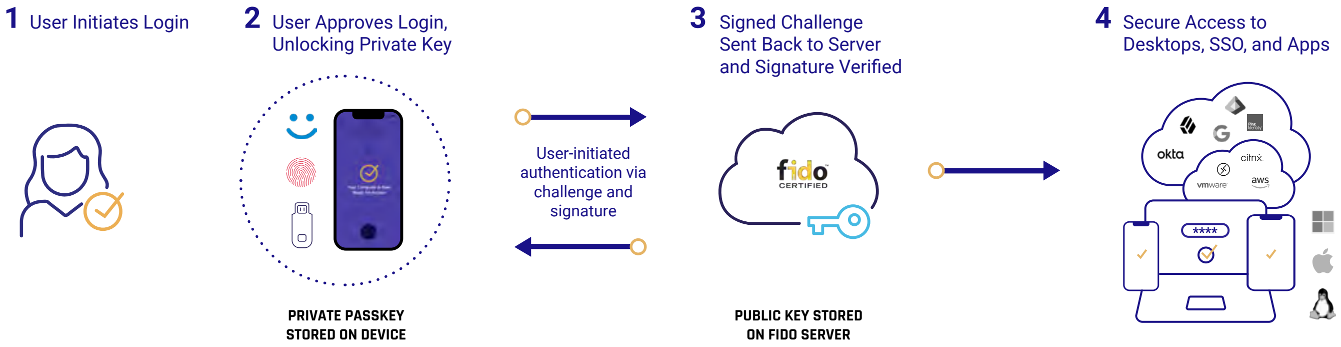
HYPR leverages deterministic controls that secure identities, even against AI-assisted cyberattacks. These include:

Strong Authentication Protocols

HYPR Authenticate is our category-leading passwordless MFA solution, which is built on top of the FIDO standards.

Cryptographic Techniques: HYPR uses public key cryptography, considered the gold standard for secure authentication. During the registration process, the user’s device creates a new public-private key pair. The private key remains secret on the device, while the public key is registered with the online service. Authentication involves proving possession of the private key without it ever leaving the user’s device, making it extremely difficult for attackers (AI-assisted or not) to steal or replicate.

Local Biometric Verification: Local biometric verification (like fingerprint sensors, facial recognition, etc.) are difficult for AI to fake because the biometric data is not transmitted over the network. Instead, the device confirms the match and then uses cryptographic keys to authenticate the user to the service.


1 User Initiates Login
2 User Approves Login, Unlocking Private Key
3 Signed Challenge Sent Back to Server and Signature Verified
4 Secure Access to Desktops, SSO, and Apps
User-initiated authentication via challenge and signature
fido CERTIFIED
okta
citrix
vmware
aws
****
PRIVATE PASSKEY STORED ON DEVICE
PUBLIC KEY STORED ON FIDO SERVER

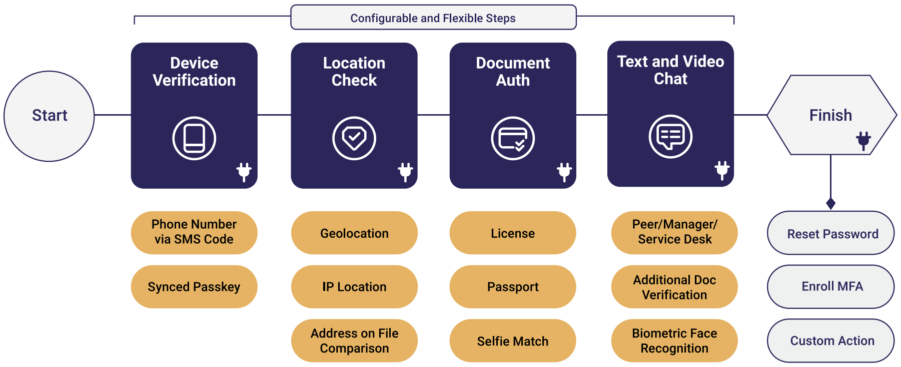
Phishing Resistance: FIDO authentication is bound to the original website's URL, making it resistant to phishing attacks. Even if AI is used to create highly convincing phishing sites, the authentication process matches the URL against the registered service's URL, preventing the credentials from being used to authenticate a fraudulent site.

Local Storage of Credentials: HYPR stores cryptographic credentials locally on the user's device. They are never shared with the server or across the network, therefore cannot be intercepted or deduced in AI-assisted attacks.

Multi-Layer Identity Verification

HYPR Affirm, our comprehensive identity verification solution, provides a deterministic way to prove people are who they claim to be. HYPR Affirm combines a series of factors such as location, behavior, document verification, face recognition, AI-powered chat, video, facial recognition and other cutting-edge technologies when verifying a user's identity. Multi-layered and highly configurable, HYPR Affirm provides advanced assurance for complex use cases, high risk events and transactions, and protects against the most vulnerable sources of cyberattacks.

HYPR Affirm User Flow



AI-Driven Identity Risk Intelligence and Mitigation

While deterministic security controls are essential, they cannot fully protect against unknown and emerging threats. HYPR Adapt integrates real-time risk assessment and adaptive security controls to manage identity-related risks, even in rapidly changing security environments. The system leverages big data, dynamically analyzing risk signals from numerous sources. This high-fidelity intelligence is used to drive automatic mitigation measures, as well as shared with SIEM, SOAR and other enterprise systems.

How HYPR Stops AI Identity Attacks

Phishing

HYPR uses strong authentication protocols based on FIDO standards, with no fallbacks to passwords or OTPs that can be intercepted or replayed. This deterministic approach to authentication eliminates credential phishing because every authentication request is initiated by the user. There is no opportunity for an adversary to prompt users to authenticate.

Impersonation via Deepfakes

Deepfakes are getting more sophisticated on a daily basis. While liveness detection is a positive step forward, it's only a matter of time before it's defeated by the rapid pace of innovation in AI. Rather than relying purely on voice or video feeds, HYPR Affirm deterministically verifies identity through a series of factors such as location, behavior, document verification, face recognition, and more.

Social Engineering

Social engineering attacks aim to induce someone to take an action, often in order for the attacker to take over the victim's account (ATO). HYPR stops social engineering on multiple fronts: victims cannot be tricked out of their credentials, impersonation attempts fail, and suspicious behaviors are flagged and blocked.

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 phishing-resistant passwordless authentication with adaptive risk mitigation, automated identity verification and a simple, intuitive user experience. With an independently validated ROI of 324%, HYPR secures some of the most complex and demanding organizations, including 2 of the 4 largest US banks, manufacturers and leading critical infrastructure companies.

HYPR

THE IDENTITY ASSURANCE COMPANY

www.hypr.com I hypr.com/contact