HYPR

HYPR SECURITY FAQ

Table of Contents

Performance and capabilities

How many transactions per second can HYPR handle?

HYPR is built to meet the dynamic needs of our clients. HYPR's system can handle thousands of transactions per second and is designed to be horizontally scalable. HYPR monitors each system to ensure capacity is not hit in customer deployments. Rigorous testing accompanies each release focusing on maintaining low response times at extremely high loads.

How does Offline Mode with HYPR work?

HYPR uses a decentralized PIN to enable offline mode. This is a pattern unique to HYPR that does not rely on a shared secret model that is centrally stored and vulnerable to attacks.

How does a user gain access when they lose their paired device?

Users can go through their organization's account recovery protocol or be issued a temporary decentralized PIN until they pair a new device with their account. Users may also leverage the HYPR Affirm product for advanced identification verification recovery processes.

What is your product support schedule?

The HYPR Product Lifecycle document delineates the support framework for various HYPR software versions, ensuring customers understand the levels of support available throughout the lifecycle of a product. This lifecycle is categorized into three distinct phases:

Standard Support Phase (1 year): This phase commences from the general availability of a software version and extends for one year. During this period, customers receive full support, including new features, enhancements, issue resolution, and critical security updates.

Limited Support Phase (6 months): Following the standard support phase, the product enters a six-month limited support period. During this phase, the focus shifts to essential support services, primarily dealing with critical issues and security updates.

No Support Phase: Post the limited support phase, the software version transitions to a 'no support' status, wherein no further updates, enhancements, or direct support services are provided.

This lifecycle approach is designed to ensure that customers can plan their upgrade and maintenance activities effectively, aligning with HYPR's commitment to providing secure, up-to-date, and efficient software solutions.

What is the availability of HYPR?

The HYPR Cloud Platform architecture is designed to ensure 99.99% availability. HYPR provides cloud-native deployments that supports high availability and is a globally distributed platform.

Does HYPR provide 24x7 support year-round?

HYPR provides a wide range of support services to cater to your specific business needs. Options include:

- Standard Support includes business-hours coverage, access to the HYPR support portal, standard troubleshooting and technical assistance.
- Premium Plus Support provides enhanced support including 24/7 coverage, with priority web and phone support, as well as technical and engineering support to ensure successful operationalization of HYPR solutions.
- Enterprise Support Package provides elevated support beyond Premium Support including phone submission, support for tailored services, annual consultation hours and access to HYPR's Admin Certification and Training Program.

For more info on our support services visit www.hypr.com/support

Integrations and Standards

How are you implementing FIDO and FIDO2?

HYPR is certified in FIDO2, UAF, and U2F standards. HYPR implements FIDO to be easily adoptable and scalable.

To learn more about FIDO, see here: https://www.hypr.com/fido-authentication.

To look up FIDO product certifications, search HYPR on the FIDO Alliance Website https://fidoalliance.org/certification/fido-certified-products/.

Does HYPR support YubiKeys and other FIDO-based security keys?

Yes, HYPR supports YubiKeys and other FIDO hardware tokens. HYPR is FIDO Certified end-to-end, making it fully interoperable with FIDO2 and U2F Certified roaming devices for passwordless or second factor authentication. These include iOS and Android mobile phones, Smart Cards and Platform authenticators (i.e. Windows Hello, and Touch ID on Apple Macbook Pro machines).

HYPR also supports CTAP. The FIDO Alliance's Client to Authenticator Protocols (CTAP1, CTAP2) specifications complement the W3C's WebAuthn Protocol, and together these protocols enable a true passwordless experience. CTAP2 enables mobile phones and FIDO security tokens to interface with FIDO2 web browsers and operating systems over USB, NFC, or BLE. Together these deliver 2FA, MFA, or passwordless authentication. CTAP1 (formerly FIDO U2F) enables existing FIDO U2F security keys and wearables for authentication on FIDO2 browser and operating systems over USB, NFC, or BLE, but only for 2FA alone.

What identity providers do you support?

Okta, Azure AD, ForgeRock, Ping Identity, FusionAuth, and any SSO provider that supports SAML or OIDC standards.

What federation frameworks do you support?

HYPR supports SAML, OAUTH2, and OIDC.

Does HYPR work with G-Suite or Office 365?

Yes, you can use HYPR with G-Suite or O365 via SAML.

Logging and Monitoring

Which SIEMs do you integrate with?

HYPR offers robust integration with a variety of SIEM tools, including popular options like Splunk, Greylog, Exabeam, and ELK. To enhance this integration, the platform enables the creation of intelligent extensions through event hooks. This feature allows for more tailored and comprehensive integration with any SIEM product in use by our customers.

For additional details on configuring these custom event hooks, please visit:
HYPR Documentation on Custom Event Hooks.

Does HYPR provide an Audit Trail? What information is logged and stored?

HYPR is designed to help administrators quickly troubleshoot when issues may occur during registration, authentication, transaction as well as de-registration. The Audit Trail functionality provides data that can be used for compliance as well as helpdesk purposes. This includes information on user devices for mobile and workstations, as well as any errors that may have occurred within the platform.

Data Management

How do you encrypt data?

Any data that is security relevant is encrypted using AES-256 encryption at rest. The encryption is done at the persistence layer within the application software.

How do you store data?

HYPR stores data in a relational database where necessary fields are encrypted.

Where do you store data?

Data protection is a top priority at HYPR. Services are provided for a variety of organizations and industries in multiple countries and strive to help customers comply with their specific geo-restriction requirements for data hosting. HYPR platform instances can be deployed into any available AWS regions depending on the customer's specific data geo-residency requirements.

How long is the data kept?

HYPR performs the following data delete operations as a part of operating the HYPR service.

- State data - user account and device information state
- All create/read/update and delete operations are performed per authoritative instruction of the data controller(customer) via service APIs or service UI. Data records are deleted in the database at row levels upon delete requests.
- Event data - user authentication and registration activity events
- Kept for the maximum of rolling 30 days (configurable to lesser duration)
- Exportable to data controllers via live Event webhooks (live) or Audit API (exportable for up to configured retention above)

Note that all data is deleted fully after the contract termination. Data may reside in backups for up-to 30 days after deletion. HYPR will notify customers in advance on any significant or material changes that affect our data retention procedures and policies

How do you provide segregation of tenant data?

Each tenant data is stored in a separate database schema in order to ensure separation of concerns for tenant information. This capability enables HYPR to easily delete, backup and restore data in the event that it's necessary. Alternative hosting segregation options are possible for additional investments.

What type of data is collected, and what PII (Personally Identifiable Information) does the product store?

HYPR primarily stores public keys which are not considered PII. HYPR also stores usernames and emails when they are used as usernames which are encrypted in the relational database. For users of the standalone HYPR Affirm product, additional PII consents and addendums provide both the enterprise and end users with the scope, collection and usage of biometric data.

Who has access to the data?

HYPR customers have direct access to their tenant's Control Center to manage their end-users and deployment configuration. HYPR Control Center supports RBAC and various federation options (SAML/OIDC) . HYPR employee access to production resources is managed through strict IAM roles and JIT access provisioning. Every individual with access to production is assigned the least privileged role unless they require additional access. In the event a user needs customer specific production access, access will be temporarily granted, with approval and access logged in an auditable way.

Who has access to data centers?

HYPR leverages AWS hosting. Please see AWS Datacenter security whitepapers, controls and compliance certifications https://aws.amazon.com/compliance/data-center/controls/.

What kind of databases do you support?

HYPR supports MySQL and JDBC-compliant databases for at rest storage. HYPR also leverages caching technologies which store temporary session data that does not require persistence.

What infrastructure is required for HYPR?

HYPR is hosted for customers on AWS. On-Premise customers can deploy HYPR on Linux or containerized systems. For Workforce Access, Active Directory Certificate Services are required in order to enable True Passwordless Desktop MFA.

Security and Privacy Certifications and Compliance

For the latest information on HYPR's certifications, visit the Security and Compliance Page.

Is HYPR SOC 2 Certified?

Yes, HYPR has certified its systems to SOC 2 Type II through an AICPA-accredited independent auditor who has assessed the operational and security processes of our service and our company.

Is HYPR ISO Certified?

Yes, an ANAB accredited auditor has certified that HYPR meets the standards for ISO 27001. This validates that HYPR has met rigorous international standards in ensuring the confidentiality, integrity, and availability of customers' information.

In addition, HYPR is certified for ISO 27017 and ISO 27018, which provide additional information security and data privacy controls for cloud service providers to protect personally identifiable information (PII) and reduce security risk in a cloud-based environment.

Does HYPR have a CAIQ and SIG completed?

Yes. For the CAIQ, please visit this website for a copy. For the SIG, please request a copy of a questionnaire from your account manager or sales contact.

Does HYPR Support SSL Pinning?

Yes, HYPR supports SSL Pinning for organizations that have it as a security requirement.

What security testing has been performed on both the HYPR Mobile App and the True Passwordless Servers that are used? Who performs this testing?

HYPR follows a strict SDLC program and does both third party and internal penetration tests and security reviews on all components including mobile applications as well as server-side software. A list or partners who have tested the HYPR platform can be found on https://www.hypr.com/trust-center/security-compliance

Does HYPR adhere to OWASP Top Ten?

HYPR follows the OWASP Top 10 and the ASVS standard for application security.

How often do you pen test your product, and office?

HYPR externally pen tests the product annually, and continually does internal pen tests for releases. Additionally, HYPR runs an ongoing bug bounty program where independent researchers continuously test our platform. Our office is in a guarded building that has security systems and cameras in place that are tested regularly.

Are you NIST 800-63B compliant?

Yes, HYPR is focused on reducing the burden on the implementation of AAL3. HYPR's solution enables businesses to be compliant regarding authentication levels of assurance known as AAL3.

Do you support the California Consumer Privacy Act (CCPA)?

HYPR addresses the 'right to deletion' as part of the CCPA. The HYPR Administrator can remove the user from specific HYPR applications they were registered with upon request.

Do you address General Data Protection Regulation (EU GDPR)?

HYPR addresses the GDPR 'right of access' to personal data and the 'right to erasure'. Upon request, administrators can supply personal data and or remove user data. HYPR also follows GDPR related practices for subprocessor requirements, alerting, storage of data and other data processing aspects. HYPR is proud to host global customers and large enterprises based in Europe counted amongst its customer list.

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.