HYPR SECURITY FAQ

HYPR.com

Table of Contents

Performance and Capabilities

How many transactions per second can HYPR handle?

HYPR scales to thousands of transactions per second. The system is horizontally scalable and handles high throughput of transactions to fit customer needs.

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.

What is your product support schedule?

HYPR provides maximum support for at least the two prior versions of the product and is actively tested across widely used builds across mobile and workstation operating systems and devices. Product updates and releases are available on a monthly basis and patches are made available as needed.

What is the availability of HYPR?

The HYPR Cloud Platform is architected to ensure 99.99% availability. HYPR provides cloud-native deployments that support 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 Support provides enhanced support including 24/7 coverage, with priority web and phone support, as well as technical and engineering support to ensure successful deployments and operationalization of HYPR solutions.
- Premium Support Plus provides elevated support beyond Premium Support including a dedicated Customer Success Manager to provide advocacy and insights as a trusted advisor.
- TAM is HYPR's highest level of support which provides customers with a dedicated Technical Account Manager who works closely with you to ensure best practice guidelines are utilized for effective deployment and operation of HYPR solutions.

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. We implement FIDO to be easily adoptable and scalable. You can learn more about FIDO 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 integrates with any SIEM tool such as Splunk, Greylog, Exabeam, ELK and more. The platform also supports the ability to create intelligent extensions that can provide further integration with any SIEM product that customers may have.

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.

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.

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.

Who has access to the data?
FIDO Control Center administrators have access, and database administrators have direct access to the data.

Who has access to data centers, how long data kept?
Only HYPR staff with proper security clearance have access to data centers. This access is regularly re-visited as part of the corporate security policy.

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 systems. For Workforce Access, Active Directory Certificate Services are required in order to enable True Passwordless Desktop MFA.

Security and Privacy Certifications and Compliance

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, A-LIGN, 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 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.

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 bi-annually, and continually does internal pen tests for releases. 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.

THE PASSWORDLESS COMPANY

Email: info.hypr.com

Learn more: www.hypr.com

HYPR fixes the way the world logs in. HYPR's True Passwordless™ multi-factor authentication (PMFA) platform eliminates the traditional trade-off between uncompromising assurance and a consumer-grade experience so that organizations decrease risk, improve user experience and lower operational costs.