Application Security
(Non-NDA)

As a Software as a Service (SaaS) offering and therefore, accessible via the public internet Hypersign has been designed with the latest security features in order to mitigate any risk to our customers and their assets.

APPLICATION SECURITY

Hypersign uses an industry standard Object Relational Model (ORM) as a protective layer between the user interface and the database. This means that there is no plain text SQL passed from the user interface to the application layer and therefore invulnerable to any type of SQL injection attack.

Hypersign uses an industry standard access control list (ACL) framework to assure user data is protected.

Hypersign prevents cross site scripting attacks by appropriately validating all user input as well as executing all URL query strings through a robust business layer.

All communication between the user and Hypersign is transferred over HTTPS using TLS 1.2 encryption. We do not service older outdated methods, such as TLS 1.1 or SSL.

INFRASTRUCTURE SECURITY

Hypersign servers are obfuscated from the Internet via load balancers and firewalls, and are only accessible from approved IP addresses (Hypersign office) via strong certificate-based authentication. Hypersign databases and servers are backed up regularly.

URLs that need to be whitelisted:

app.hypersign.net
util.hypersign.net
https://assets.hypersign.net/

Hypersign internet traffic commutes through ports 80 and 443.

DATA SECURITY

Hypersign does not request or store PCI, PHI, Sensitive PII, or any other sensitive data.