

Benefits

Secure Communications with IPSec VPN

256-bit encryption for private communications between your enterprise and our servers hosted by AWS for secure services.

Enable Secure Access to Cloud Resources

Protecting stationary data as well as data in motion.

Third-Party Compliance Assessments

We regularly pass rigorous third-party compliance assessments by HOTB Secure Solutions.

Hiper Hipo Data Security

The Data Security Challenge

The challenge for many organizations and cloud services is protecting data not only when the data is stationary, but also when data is in motion. One of the top priority for many organizations is being able to extend their datacenter out into the cloud to leverage different cloud services to reduce their total cost of ownership for those services that benefit their business while protecting their data assets. However, data assets move through the cloud in different ways and organizations struggle to extend their security perimeter preventing the different threats associated to intrusion.

The Hiper Hipo Solution

Securing client data is a top priority. Our strong security posture protects the privacy and integrity of your data across our platform. Hiper Hipo's data solution enables secure access to cloud resources through secure tunnels. Hiper Hipo utilizes 256-bit encryption to secure tunnels between our clients and our colocation partner AWS. Secure user sessions are authenticated to support security compliance. Hiper Hipo's security practices and protocols include the use of firewalls, intrusion detection and event monitoring devices, SSL certificates for secure web traffic and 256-bit database encryption data both in transit and at rest. On top of AWS robust security model and Hiper Hipo's strong security posture, Hiper Hipo leverages HOTB security solutions to perform annual network and application penetration tests to review and assess business policy and procedures, workflow, technology infrastructure and software security.

Hiper Hipo's back-up systems contain customer information and are fully maintained and tested on a regular basis in order to minimize the risk of system failures and unauthorized access or intrusions. As part of its contingency planning, Hiper Hipo has established disaster recovery and business resumption measures applicable to customer information that may result from (i) environmental failure (e.g., water, smoke, fire damage), (ii) technological failure (e.g., power outage, system malfunction), including the availability of backup power supply to guard against possible electrical outages, or (iii) other events or occurrences beyond Hiper Hipo's control (e.g., floods, riots, hurricanes). These measures are designed to allow recovery of any customer information that may have been affected by an environmental, technological, or other failure and to provide continued servicing of client needs. Controls are also in place to protect against fraud, theft, and employee dishonesty.

Hiper Hipo performs unit testing, regression testing, automated load testing and penetration testing as part of its product delivery process. We utilize staging and pre-production testing environments during our stages of testing. Hiper Hipo does not build "back-doors" into its product. Hiper Hipo builds and continually updates, rigorous safeguards into every product to maintain the highest security and maximum uptime.