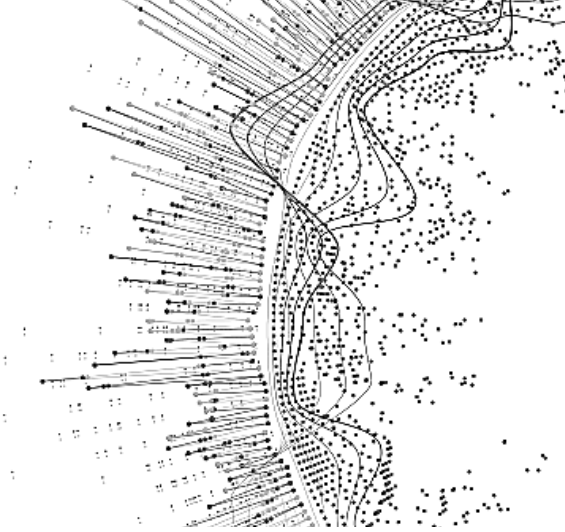
ENTERPRISE-GRADE SECURITY TO HELP PROTECT YOUR DATA AND MEET YOUR COMPLIANCE REQUIREMENTS

Ospree takes your data security seriously, and the platform includes a robust set of security and data protection product features that give you the control, visibility and flexibility you need to manage all your security challenges, without compromising agility.



Identity and Device Management

Securing your information starts with identity controls, no matter where your users are located. Ospree allows you to manage users and groups, and assign roles and permissions. We give you the power to ensure that only the authorized people can access your company's information in the Ospree application.

- Session duration
- Two-factor authentication
- Fully auditable privileged access controls

Data Protection

By default, Ospree encrypts data at rest and in transit as part of our foundational security controls.

- All connections to the platform are protected with enterprise-grade TLS encryption.
- All data is encrypted at rest and stored in a secure data center.

Data Retention Policy

Ospree will retain customer data for expired accounts for a minimum of 6 months, after which it is subject to deletion. In the event that the customer initiates an account deletion, the relevant data will be removed within 30 days, except where it may be required to be retained for a longer period in order to comply with a legal obligation.

Data Storage and Disaster Recovery

Customer Data is backed up and stored redundantly at multiple locations in our hosting provider's data centers to ensure availability. Our well-tested backup and restoration procedures allow recovery in the event of hardware failure. Customer Data and our source code are automatically backed up nightly. Backups are fully tested at least every 180 days to confirm that our processes and tools work as expected.

- Nightly backups
- Redundant backups
- Periodic disaster recovery drills

Data Centers

Ospree only uses the highest-rated data centers that meet or exceed some of the most stringent and most broadly recognized security standards, including but not limited to:

- ISO 27001
- ISO 27017
- ISO 27018

Datacenter Locations:

- Singapore
- United States
- Germany
- Australia

Contact ospree.io/get-demo to learn more.

ospree