MAINTAIN SECURITY AND COMPLIANCE WITH OCIENT

In an era marked by increasingly large datasets full of important and sensitive data, data breaches have more potential implications than ever before. As the leading data analytics platform for always-on, compute-intensive analytics, Ocient supports customers' data security from multiple angles. From security considerations built directly into the Ocient Hyperscale Data Warehouse™ to a comprehensive internal security program and annual recertifications, Ocient is committed to making data security a priority.

Built on a bedrock of security

To build the Ocient Hyperscale Data Warehouse, Ocient's team of engineers went back to basics, rethinking the way businesses use NVMe SSDs to process data. This paved the way for some very impressive performance improvements, plus it provided an opportunity to build in security at every step. All Ocient systems benefit from the following security features:

Role-based access control. Ocient's system-wide access control enables administrators to limit user access according to needs and roles.

Ingestion privacy. Masking or hashing data at ingest offers an additional level of protection, keeping sensitive data off the Ocient platform entirely.

View curation. With Ocient, customers can create views that limit, transform, or mask information to minimize data exposure.

Audit logging. The Ocient system can create logs of user authentication activities, permission changes, and more, then automatically share them with log analysis tools.

COMPLIANT WITH KEY SECURITY AND PRIVACY STANDARDS

GDPR COMPLIANT

The Ocient Hyperscale Data Warehouse provides customers with the capabilities they need to comply with the General Data Protection Regulation (GDPR), which applies to any business that processes data associated with citizens or residents of the EU or the UK.

CCPA READY

The Ocient Hyperscale Data Warehouse provides customers with the capabilities they need to comply with the California Consumer Privacy Act (CCPA), which applies to any business that processes data associated with California residents.

AICPA SOC 2

Solutions deployed in the OcientCloud® or managed by Ocient Management Services are certified annually to AICPA SOC 2 Type II.

© Ocient2025

FLEXIBLE DEPOYMENT OPTIONS

Choose the deployment modality that works best for your business and security needs

On Premises
Deployed on commodity hardware in your datacenter

Public Cloud
Amazon Web Services, Google Cloud Platform, or Oracle Cloud

OcientCloud
Hosted in the Ocient datacenter

Ocient Management Services: Lighten the Load

Let our our experts manage your deployment, helping with software installation, upgrades, and more so you can focus on more pressing business priorities. Ocient Management Services can also provide 24x7 system monitoring and reporting.

DELIVERING SECURE DEPLOYMENTS AND SERVICES

In addition to the built-in security features of the Ocient Hyperscale Data Warehouse, customers who deploy on OcientCloud or engage Ocient Management Services get the added peace of mind that comes with:

Comprehensive Internal Security Program
- AICPA SOC2 TYPE II compliant services
- Third-party penetration testing
- Personnel security program

Data Encryption
- Data-in-transit and data-at-rest encryption
- Direct connects to major public clouds
- System auditing/monitoring

Access Management
- Multi-factor authentication
- IP allowlists
- Restricted access to OcientCloud facility

Physical Security
- Environmental and physical security monitoring
- OcientCloud is hosted in SOC 2, ISO 27001, ISO 22301, DC OIX-2, HITRUST, PCI DSS, and FISMA-compliant data center

Ready to learn more?

Contact our sales team: sales@ocient.com

© Ocient 2025