Frequently Asked Questions for IT & Procurement Leaders

Where is Omnant hosted, and what is the architecture?
All systems are hosted at Amazon Web Services (AWS) in the US West 2a region. Each client instance is hosted independently -- no data is shared between instances. The core of the Omnant platform is a web application supported by microservices and data stores, all developed within the Microsoft .NET Framework. Supporting infrastructure can be scaled based on the needs of each instance.

What programming languages and technologies are used?
All components of Omnant are developed in the Microsoft .NET Framework and other applications within the Microsoft ecosystem. Data is stored in Microsoft SQL Server databases and in private S3 buckets at AWS.

Do you support Single Sign-On (SSO)?
Yes. Omnant supports SSO via OIDC with any provider, including Okta, Office 365, and Google Workspace. There is a one-time setup fee with discounts available when multiple instances are required.

Does Omnant support multi-factor authentication (MFA)?
Yes. MFA can be enforced for all users through the web interface. When using SSO/OIDC, your IT department controls MFA enforcement. For Omnant-managed authentication, users can be required to enable MFA.

How is data kept secure and separate between Omnant's clients?
Each client's data files are stored in two dedicated, independent locations: a private S3 bucket and a Microsoft SQL Server database. No data are shared between instances.

Do you encrypt data at rest and in transit?
Yes. All data are transmitted via HTTPS. SQL Server databases use Transparent Data Encryption (TDE). All database backups are stored in compressed, password-protected archives.

Contact Us

(312) 436-1529 omnant.com

What are your data backup and recovery procedures?
Data are backed up off-server every 15 minutes, with full nightly backups. The 15-minute backups are restorable for 30 days and nightly backups are retained for 365 days. The backup software tests and validates each backup automatically. Our target Recovery Time Objective (RTO) is 4 hours under normal operating conditions. Our Recovery Point Objective (RPO) is 15 minutes, aligned with our backup frequency. These targets assume AWS infrastructure availability; in the event of a regional AWS outage, recovery timelines would depend on AWS restoration.

Do you support API access for data import and export?
Yes. Omnant provides a RESTful API that supports core functions including accessing approved reports, pushing and pulling break data, and managing project documents. API capabilities are expanded on an ongoing basis as client needs are identified.

Do you have an incident response plan?
Yes. The plan covers preservation of customer data confidentiality, defined personnel responsibilities, and processes for each stage of an incident lifecycle: identification, notification, containment, and recovery. Incidents are detected through periodic environment scans and employee reporting. In the event of a confirmed breach affecting your data, we notify affected customers directly via email and phone as soon as the incident has been assessed, with details on what occurred, what data was affected, and remediation steps underway. No security incidents have occurred since the company was founded.

Are you compliant with SOC 2 or ISO 27001?
Omnant does not currently hold formal third-party certifications for SOC 2 or ISO 27001. Our information security policies incorporate components of both frameworks and are reviewed at minimum annually and after any material change to the technology stack. We are happy to discuss our specific controls in more detail.

Do you comply with GDPR or CCPA?
We do not currently maintain a formal GDPR or CCPA compliance program. We do not share or sell any client data to third parties. The only personal data we store is name and email address. We are happy to detail how we handle your organization's specific data upon request.

How do you manage vulnerability patching and security testing?
Third-party libraries and dependencies are reviewed and patched on a bi-monthly basis. Server-level patches are applied monthly. We leverage AWS security tooling and configurations for continuous runtime monitoring, supplemented by IP and port restrictions on critical infrastructure. Code security is maintained through peer review prior to merging. We do not currently perform standalone penetration tests or use formal SAST/DAST tooling, but we are evaluating automated code analysis options as part of our ongoing security program development.

Who on your team has access to our data, and how is that access controlled?
Customer data access is available to our support team, each of whom plays a cross-functional role in product, support, and operations. Access requires MFA and all activity is logged at the application level. Access permissions are reviewed as part of any staff change. We do not currently implement time-bound access windows.

What sub-processors does Omnant use?
Omnant's current sub-processors are AWS (hosting infrastructure), Twilio (SMS messaging), Atlassian (internal project management), and SigNoz (monitoring). On the customer side, your email provider and optional SSO provider would also be involved in the workflow, but those are managed by your organization.