Infrastructure Q&A

Upgrades and Maintenance

Does your service have regular maintenance windows, and if so, what are they? What services are impacted or unavailable during these times?

AWS monitors electrical, mechanical, and life support systems and equipment to help ensure immediate identification of any issues. In order to maintain the continued operability of equipment, AWS performs ongoing preventative maintenance.

Logging and System Management

Explain what configuration options your solution provides for logging end-user and administrator actions. Please address the general types of events that can be logged (or not logged), options for setting formatting and logging levels, options for setting retention policies, purging, and so on.

On top of standard AWS tools we're using, we do not log any sensitive data.

Hosting Infrastructure, Backup and Disaster Recovery

Please describe the types of data center facilities in which your solution is located.

Detailed information can be found in the Security Overview.

Please list any 3rd party audit of the data center facilities and the frequency they are audited.

All the details can be found in the AWS security whitepaper.

What are the Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for MWA data?

We're using RDS services with a few database instances. Data is backed up on a daily basis.

Integration, Data Import, Export and Location

What does your solution support for exchanging structured information both into and out of your system? Explain the general mechanism and standards supported.

We're using JSON and SFTP. All the CMS data is being processed via HTTPS.

Architecture and Supported Platforms

What client PC/laptop operating systems and browsers does your solution support? Differentiate by OS version if/where appropriate.

We support all modern operating systems and browsers.

What client smartphone and tablet operating systems does your solution support? Differentiate by smartphone and tablet OS version if/where appropriate.

We support all modern smartphone and tablet operating systems.

Security

Describe your Single Sign-On (SSO) capabilities. What types of SSO mechanisms can you support? Are there any SSO variations you cannot support?

Treepl has its own custom developed SSO that is supported and constantly updated by in-house developers. You may request integration with 3rd party customer login as well.

For client-side implementations of your solution (including browser version, offline-access version if applicable, tablet and smartphone versions if applicable), what data is cached client-side? How is such data deleted or otherwise managed at session termination? If the answer differs for each solution, please provide all relevant responses.

Static files are being cached, more information is coming soon.

Do you require the use of two-factor authentication for the administrative control of servers, routers, switches and firewalls?

Treepl CMS uses Multi-Factor Authentication (MFA), Secure Shell (SSH) and Secure Sockets Layer (SSL) for management connections to manage the AWS infrastructure.

Does your solution support TLS 1.2 (or other industry-standard transport security) with encryption and two-factor authentication for connecting to the application?

We support TLS 1.2 and 2FA for the sites administration.

Policy Review

Please provide a copy of your information security and privacy policies.

Detailed information can be found in the Security Overview and Privacy Policy.

Please provide a copy of your access control and identity management policies.

Detailed information can be found in the Security Overview.

Please provide a copy of your disaster recovery and business continuity policies and procedures.

Detailed information can be found in the Security Overview.

Please provide a copy of your systems and network security policies.

Detailed information can be found in the Security Overview.

Please provide a copy of your patch management policy.

AWS maintains responsibility for patching systems that support the delivery of AWS services, such as the hypervisor and networking services. Treepl CMS is responsible for patching its guest operating systems (OS), software, and applications running in AWS.

Please provide a copy of your vendor and third-party service provider management policies.

Detailed information can be found in the Terms of Service.

Please provide a copy of your incident response policy.

Detailed information can be found in the Incident Response Plan.

Please provide a copy of your breach notification policy.

Detailed information can be found in the Incident Response Plan.

Development Environment

Please describe your development and quality assurance environments, including vulnerability scanning tools.

CI/CD process using Jenkins. No vulnerability scanning at the moment.

Please describe your use of any third-party developers. Please indicate the location of those developers (country).

100% of Treepl CMS specialists that are granted any level of access to Treepl CMS assets are in-house employees. We do not outsource any type of work to 3rd parties or contractors.

Secondary (Non-Production) Environments

Do you provide customers with a standard set of secondary non-production environments (staging, test, and so on)? If so, which types of environments? Are there any limitations on access to and usage of these environments?

We provide our clients with trial sites for developing sites and testing purposes.

Is any MWA data exposed or used in any environment, other than production? (development, test, staging, QA, etc.)

We can do this on client's request to troubleshoot the bugs.

If you have a multi-tenant architecture that extends to the database level, describe the set of controls for ensuring the separation of data and the security of information between different customers' instances?

Treepl CMS data stored on AWS includes strong tenant isolation security and control capabilities. As a virtualized, multi-tenant environment, AWS implements security management processes and other security controls designed to isolate each customer, such as Treepl CMS, from other AWS customers. AWS Identity and Access Management (IAM) is used to further lock down access to compute and storage instances.

Data Storage/Usage

Please indicate if MWA data in your solution is ever stored or moved outside the US, and if so what type of data is stored outside the US (e.g. images, cached data, data in transit).

The sites deployed in the US are stored in the US.

Does your solution encrypt production databases and file shares? Are system/data backups encrypted?

We're using XTS-AES-256 for data at rest and ECDHE, DHE, RSA, AES for data in transit.