Treepl CMS Security Overview

About Treepl CMS

Treepl CMS is an all-in-one business website and online marketing solution providing an integrated platform for Content Management (CMS), Customer Relationship Management (CRM), Email Marketing, Ecommerce and data analytics.

Treepl CMS Architecture & Amazon Web Services

Treepl CMS is fully hosted in Amazon Web Services (AWS) and it takes advantage of a large set of its products: Amazon Elastic Compute Cloud (EC2) for scalable computing capacity in the cloud, Elastic Block Store (EBS) and Simple Storage Service (S3) for storing and retrieving data, Virtual Private Cloud (VPC), Identity and Access Management (IAM), Security Groups, and others for security purposes, Simple Email Service (SES) for sending emails, CloudWatch for monitoring, and others.

In order to obtain a higher performance level, Treepl CMS customers are hosted and served from five AWS data centers: Germany (EU), Oregon (US), Sydney (AU), Canada (CA), United Kingdom (UK).

AWS offers a reliable platform for software services used by thousands of businesses worldwide, provides services in accordance with security best practices, and undergoes regular industry-recognized certifications and audits. More information can be found in the *AWS Security White Paper*.

Operational Responsibilities of AWS and Treepl CMS

AWS operates, manages, and controls the components from the hypervisor virtualization layer down to the physical security of the facilities in which Treepl CMS operates. In turn, Treepl CMS assumes responsibility and management of the guest operating system (including updates and security patches) and application software, as well as the configuration of the AWS-provided security group firewall.

AWS also operates the cloud infrastructure used by Treepl CMS to provide a variety of basic computing resources, including processing and storage. The AWS infrastructure includes facilities, network, and hardware, as well as operational software (e.g., host OS, virtualization software, etc.), which supports the provisioning and use of these resources. AWS is designed and managed according to security best practices as well as a variety of security compliance standards.

Geographic Location of Customer Data on AWS Network

Except for very little operational information (e.g., DNS entries), customers' data is stored exclusively in the designated AWS region/data center. Content that customers store in Treepl CMS (e.g., assets) is not replicated to other data centers in other regions.

Isolation of Customer Data/Segregation of AWS Customers

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.

Secure Network Architecture

AWS employs network devices, including firewall and other boundary devices, to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services. ACLs, or traffic flow policies, exist on each managed interface to manage and enforce the flow of traffic. Amazon Information Security approves all ACL policies and automatically pushes them to each managed interface using AWS's ACL- a management tool, helping to ensure these managed interfaces enforce the most up-to-date ACLs.

Network Monitoring and Protection

AWS uses a variety of automated monitoring systems to provide a high level of service performance and availability. Monitoring tools help detect unusual or unauthorized activities and conditions at ingress and egress communication points.
The AWS network provides significant protection against traditional network security issues:
• Distributed Denial Of Service (DDoS) Attacks
• Man in the Middle (MITM) Attacks
• IP Spoofing
• Port Scanning
• Packet sniffing by other tenants

You can find more information about Network Monitoring and Protection in the AWS Security Whitepaper on the Amazon website.

Service Monitoring

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.

Data Storage and Backup

Treepl CMS stores data in Amazon EBS and backs it up via snapshot lifecycle policies every 12 hours.

Change Management

AWS authorizes, logs, tests, approves, and documents routine, emergency, and configuration changes to existing AWS infrastructure in accordance with industry norms for similar systems. Amazon schedules updates to AWS to minimize any customer impact. AWS communicates with customers, either via email, or through the *AWS Service Health Dashboard* when service use is likely to be adversely affected. Treepl CMS also maintains a similar status page.

Patch Management

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.

AWS Data Center Physical and Environmental Controls

AWS physical and environmental controls are specifically outlined in a SOC 1, Type 2 report. The following section outlines some of the security measures and controls in place at every AWS data center around the world. You can find more detailed information about AWS and Amazon's security controls on the Amazon security website.

Physical Facility Security

AWS data centers utilize state-of-the-art, innovative architectural and engineering approaches. Amazon applied its many years of experience designing, constructing, and operating its own large-scale data centers to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities, and Amazon strictly controls physical access both at the perimeter and at building ingress points using professional security staff, video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if he or she continues to be an

employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

Fire Suppression

AWS installs automatic fire detection and suppression equipment in all AWS data centers. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Controlled Environment

AWS employs a climate control system to maintain a constant operating temperature for servers and other hardware, preventing overheating and reducing the possibility of service outages. AWS data centers maintain atmospheric conditions at optimal levels. AWS personnel and systems monitor and control both temperature and humidity at appropriate levels.

Backup Power

AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, 7 days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

Video Surveillance

Professional security staff strictly controls physical access both at the perimeter and at building ingress points for AWS Data Centers using video surveillance, intrusion detection systems, and other electronic means.

Disaster Recovery

AWS data centers include a high level of availability and tolerate system or hardware failures with minimal impact. Built-in clusters in various global regions, all data centers remain online 24/7/365 to serve customers; no data center is “cold”. In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites. You can find more information about AWS disaster recovery protocols on the Amazon Security website.

Treepl CMS Authentication

When creating a free or paid signup on treepl.co website, users must create a Treepl CMS account, which is used every time they access the Treepl Portal and/or their individual sites.

Treepl CMS account leverages a strong hash algorithm for passwords. Treepl CMS continually monitors Treepl CMS accounts for unusual or anomalous account activity and evaluates this information to help quickly mitigate threats to the security of your Treepl CMS account. Additional security is utilized if multiple consecutive failed login attempts occur upon attempting to gain access to the admin console of a Treepl CMS site. After several failed attempts, the account's login ability is blocked for a few minutes, if failed attempts continue, block window grows to prevent brute force attacks. Upon a successful login attempt, the user's username and password are verified through a secure connection utilizing a 256-bit SSL certificate and then redirected to their site's admin console.

Customers have the ability to secure sensitive web pages and content behind a secure zone. A secure zone will require a visitor to log in with a username and password in order to gain access. A user can initiate password restoration for a customer account, resulting in email with a link to restoration being sent to a customer email. Passwords can be restored only using a unique token provided in the email.

Payment gateway information is updated through the admin console. The page that facilitates this is served over HTTPS, as do all pages, as Treepl CMS utilizes mandatory HTTP to HTTPS redirect. Therefore, whenever a customer submits a payment, the payment is also always processed over HTTPS. HTTPS is secured via an SSL connection utilizing a 256-bit SSL certificate. Treepl CMS uses Let's Encrypt as a certificate provider. All trial and live sites are automatically set up with certificates that are valid for 3 months and are automatically renewed.

Secure Management

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

Treepl CMS Corporate Locations

Treepl CMS development and administration team is based in Kharkiv, Ukraine and implements the following processes and procedures to protect the company against security threats:

Physical Security

Treepl CMS office employs on-site guards to protect the premises 24/7. Treepl CMS employees carry a key card ID badge for building access. Visitors enter through the front entrance, sign in and out with the receptionist, display a temporary Visitor ID badge, and are accompanied by an employee at all times. Treepl CMS keeps most of its resources in the cloud, including development and staging environments, mail, code repositories etc. Personal machines are always password-locked and devices holding crucial data are additionally encrypted, with access being available only to authorized staff members.

Treepl CMS Employees

Employment Policy

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

Employee Access to Customer Data

Treepl CMS maintains segmented development and production environments for CMS, using technical controls to limit network and application-level access to live production systems. Employees have specific authorizations to access development and production systems.

Background Checks

Treepl CMS obtains background check reports for employment purposes. The specific nature and scope of the report that Treepl CMS typically seeks includes inquiries regarding educational background; work history; court records, including criminal conviction records; and references obtained from professional and personal associates, each as permitted by applicable law.

Employee Termination

When an employee leaves Treepl CMS, the employee's manager submits an exiting worker form. Once approved, HR initiates an email workflow to inform relevant stakeholders to take specific actions leading up to the employee's last day. In the event that Treepl CMS terminates an employee, HR sends a similar email notification to relevant stakeholders, including the specific date and time of the employment termination.

IT then schedules the following actions to help ensure that, upon conclusion of the employee's final day of employment, he or she can no longer access Treepl CMS confidential files or offices:

- Email Access Removal
- Remote VPN Access Removal
- Office Badge Invalidation
- Network Access Termination

Upon request, managers may ask building security to escort the terminated employee from the Treepl CMS office or building.

Customer Data Confidentiality

Treepl CMS always treats customer data as confidential. Treepl CMS does not use or share the information collected on behalf of a customer except as may be allowed in a contract with that customer and as set forth in the Treepl CMS Terms of Service.

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of the Treepl CMS platform. At Treepl CMS, we take the security of your digital experience seriously.

For more information

Treepl CMS security:
treepl.co/security-overview

Treepl CMS privacy:
treepl.co/privacy-policy

Treepl CMS terms of service:
https://treepl.co/terms-of-service