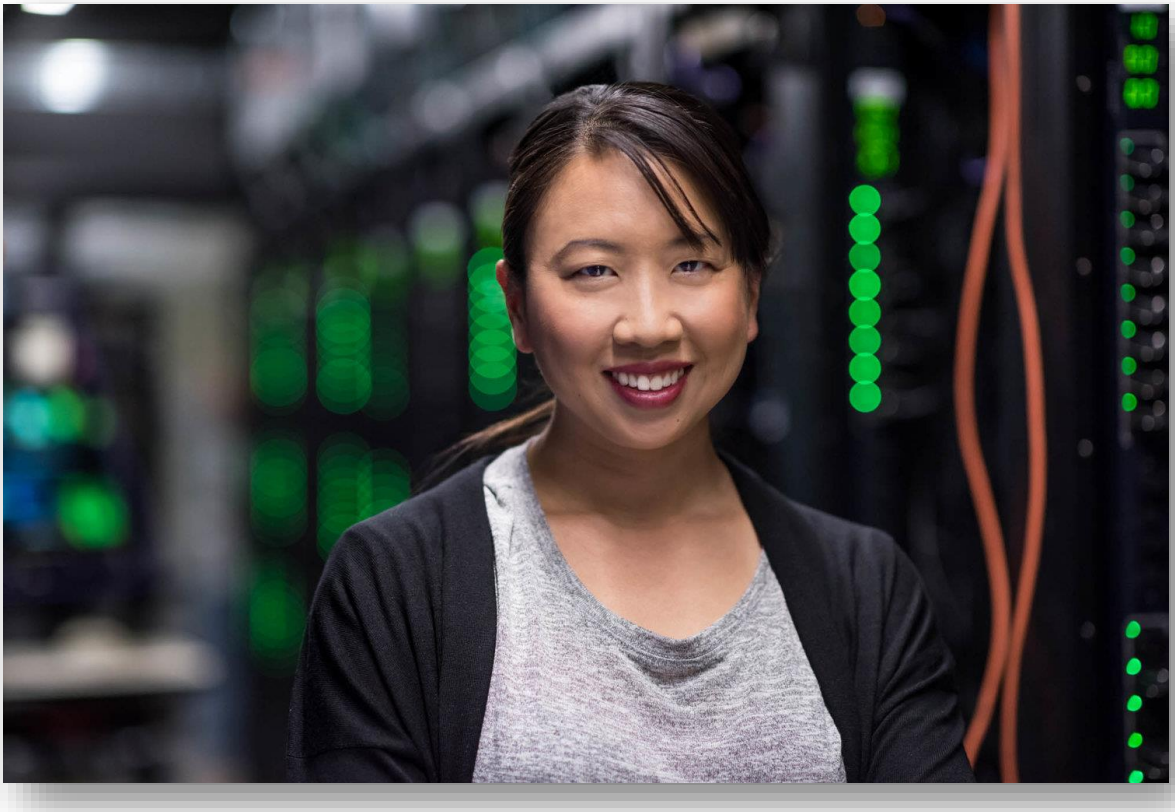

Security Whitepaper

Our Mission

Relationships are the backbone of the world's most vital industries but managing them is far from a perfect science. JungleWP is on a mission to revolutionize the underlying tools and processes to better help your business scale WordPress for million users globally. To do so, we need to make sure your data is secure; protecting it is one of our most important responsibilities. JungleWP has designed platforms and applications to meet these requirements as well as exceeded relevant industry security protocols and standards by complying to our partners Security governance and rules. We are committed to being transparent about our security practices and helping you understand our approach.

Table of Contents

People Security

All JungleWP employees are required to understand and follow internal policies and standards. Background checks are performed to screen all employees. Security training is mandated as part of the onboarding process. Topics covered include device security, acceptable use, preventing spyware/malware, physical security, data privacy, account management, and incident reporting, among others.

Application Security

Secure Software Development Lifecycle

Standard best-practices are used throughout our software development cycle from design to implementation, testing, and deployment. All code is checked into a permanent version-controlled repository. Code changes are always subject to peer review and continuous integration testing to screen for potential security issues. All changes released into production are logged and archived, and alerts are sent to the engineering team automatically. Access to JungleWP/clients applications source code repositories requires strong credentials and two-factor authentication.

Secure by Design

All features and services access are reviewed by a team of senior engineers as soon as they are conceived. Members of the JungleWP team have substantial experience working with and building secure technology systems. We believe in secure by design, hence we plan all functionalities with security in mind to protect the platform against security threats and privacy abuses.

We leverage modern browser protections, such as Content Security Policy (CSP) and security HTTP headers to prevent Cross-Site Scripting (XSS), Clickjacking and other code injection attacks resulting from the execution of malicious content in the trusted web page context.

Security Testing

Once features are implemented, we perform internal security testing to verify correctness and resilience against attacks. We follow the leading Open Web Application Security Project (OWASP) Testing Guide methodology for our security testing efforts. Discovered vulnerabilities are promptly prioritized and mitigated. In addition, we regularly engage top-tier third-party security companies to independently verify our applications.

Authentication

JungleWP allows users to login to our services by using OAuth 2.0, the industry standard for authorizing secure access to external apps without exposing their account credentials. JungleWP does not receive or store user passwords when using OAuth. We implement the most secure version of the OAuth 2.0 authorization code grant to mitigate attacks that could leak the user's access token. Both access tokens and refresh tokens are encrypted at rest using AES-128 encryption. We also do not retain user access, every access shared with us to perform our work are immediately deleted after our work is complete.

JungleWP also allows users to access their server resources by using strong SSH keys, services access use strong password hash. We encrypt the credentials at rest using AES-128 encryption and in transit using Secure Sockets Layer (SSL)/Transport Layer Security (TLS 1.2). The credentials are only used to verify login .

All the above authentication flows have been extensively tested against common attacks including but not limited to Cross-Site Request Forgery (CSRF) and misconfigurations of the redirect url by an independent security testing company. Users can further revoke access from JungleWP at any time and request all their data in JungleWP to be deleted.

Network Security

Encryption in transit

To protect data in transit between JungleWP's apps and our servers, JungleWP uses SSL/TLS during data transfer, creating a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption. SSL/ TLS is further used to encrypt the traffic between JungleWP servers and JungleWP databases within the same datacenter. JungleWP monitors the changing cryptographic landscape and upgrades its cipher suite settings as the risks change.

In our web application, we flag all authentication cookies as *Secure* and enable *HTTP Strict Transport Security (HSTS)* with "*includeSubDomains*" and "preload" enabled. Our web domain is included in the HSTS Preload list for all major browsers which is maintained at https://hstspreload.org/ Together with SSL/TLS and JungleWP public certificates, HSTS prevents man-in-the-middle attacks and ensures that JungleWP apps only communicate with JungleWP servers.

Network Isolation

JungleWP divides its systems into separate networks using logically isolated Virtual Private Clouds in Amazon Web Services data centers. This setup protects sensitive data by providing isolation between machines in different trust zones. Systems supporting testing and development activities are hosted in a separate network from systems supporting JungleWP's production website. Customer data only exists and is only permitted to exist in JungleWP's production network, its most tightly controlled network.

Network access to JungleWP's production environment from open, public networks (the Internet) is significantly restricted. Only network protocols essential for making JungleWP's service work are open at JungleWP's perimeter. All network access between production hosts is restricted using security groups to only allow authorized services to interact in the production network.

Our infrastructure and applications are monitored using standard health checks and log watchers. This helps detect systems that are malfunctioning as well as potential intrusions. Our on-call engineering team is responsible for investigating and addressing issues as they emerge.

Physical Security

Data center security

JungleWP leverages Amazon Web Services (AWS) data centers for all production systems and customer data. AWS offers state-of-the-art physical protection for the servers and complies with an impressive array of standards. For more information on AWS Data Center Physical Security, see the AWS Security Whitepaper: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

Office and Digital Equipments Security

A set of policies and procedures have been implemented to address the security posture of our workstations and laptops. All employee computers comply with these standards for device security. We require computers to have strong passwords, full disk encryption and automatic lock when idle. Even though no data is stored on employee computers or servers located in our office, JungleWP's premises are protected with locked building entrances, deadbolted doors, CCTVs, and intrusion detection alarms.

Data Security

We are committed to the goals of confidentiality, integrity, and privacy of our customer data by employing a multifaceted approach to data security.

Encryption at rest

All data at rest in JungleWP's production network is encrypted using 256-bit Advanced Encryption Standard (AES). JungleWP leverages AWS Key Management Service (KMS) to manage encryption keys. Keys are never stored on disk, but are delivered at process start time and retained only in memory while in use. The most sensitive customer data such as email bodies and access tokens are further encrypted in our database and in-memory storages such that the plaintext never exists on JungleWP databases at any point in time. To ensure the security of our database, encryption keys are rotated regularly.

Employee Access to Customer Data

No customer data persists on employee laptops. We apply the principle of least privilege in all operations to ensure confidentiality and integrity of customer data. All access to systems and customer data within the production network is limited to those employees with a specific business need. A best effort is made to troubleshoot issues without accessing customer data; however, if such access is necessary, all actions taken by the authorized employee are logged. Upon termination of work at JungleWP, all access to JungleWP systems is immediately revoked.

Audit Trails

All actions taken to make changes to the infrastructure or to access customer data for specific business needs are logged for auditing purposes. In order to protect end user privacy and security, only a small number of senior engineers on the infrastructure team have direct access to production servers and databases.

Employee Authentication

Every JungleWP employee is provided with a secure password manager account and is required to use it to generate, store, and enter unique and complex passwords. The use of a password manager helps avoid password reuse, phishing, and other behaviors that reduce security. All access to the production servers and data is protected using network isolation and strong authentication mechanisms. A combination of strong passwords, passphrase-protected SSH keys, a Virtual Private Network (VPN), and two-factor authentication is used to shield mission critical systems.

Server Hardening

Servers deployed to production, as well as bastion hosts used to access production servers, are hardened by disabling unnecessary and potentially insecure services, removing default passwords, and applying JungleWP's custom configuration settings before use. We setup our systems following the Center for Internet Security (CIS) Benchmark recommendations. CIS Benchmarks are consensus-based configuration guidelines developed by experts in US government, business, industry, and academia to help organizations assess and improve security.

Vulnerability Management

JungleWP works with third-party independent vendors to perform automated vulnerability tests and manual pentesting on our production environments. We also tap into the broader security community via a private bug bounty program and offer incentives for researchers to responsibly disclose software bugs and centralize reporting streams. This involvement of the external community provides an independent scrutiny of JungleWP applications to help keep users safe. Engineers are always on call to immediately address any discovered threats to our network.

We support vulnerability disclosure by taking responsibility for addressing product vulnerabilities in a timely manner, And we work relentlessly with partners and community members to always stay on top of the newest vulnerabilities discovered in WordPress Plugins, Themes, Core or stack applications.

Compliance

Compliance with applicable regulations, standards and industry best practices protect us and our customers' sensitive information in ways that are testable and verifiable. The following security-related audits and certifications are applicable to JungleWP services:

- **General Data Protection Regulation (GDPR):** JungleWP has introduced tools and processes to ensure our compliance with requirements imposed by the GDPR.

- JungleWP Infrastructure is hosted in Amazon Web Services (AWS) data centers and Digital Ocean Datacenter, which are highly scalable, secure, and reliable. AWS and Digital Ocean comply with leading security policies and frameworks, including SSAE 16, SOC framework, ISO 27001 and PCI DSS. More information can be found at https://aws.amazon.com/compliance/ and https://www.digitalocean.com/legal/certifications/.

Privacy features

JungleWP is built upon being able to view and understand how your team interacts with other people and companies. As such, JungleWP provides various visibility features with conservative defaults that allow users to control how much information is shared with their team. Below is a small sample of such features:

Hidden Persons

Users can choose to hide, from their entire team, all email and event interactions between their team and any person(s) as well as all profile information about that person(s).

Email Visibility

By default, email bodies are only viewable by users who sent or received those emails. Email subjects, email recipients, event titles, and event invitees are viewable by all team members. However, users can choose to hide these from all team members as well.

List Sharing

By default, a new list created by a user is only visible to that user (also known as the owner of that list). The owner can choose to let specific team members or the entire team view and manage the settings for that list.

The JungleWP Privacy Policy can be viewed at https://docs.junglewp.com/article/35-data-privacy

Disaster Recovery and Business Continuity

JungleWP customer data is regularly backed up each day to guard against data loss scenarios. All backups are encrypted both in transit and at rest using strong industry encryption techniques. All backups are also geographically distributed to maintain redundancy in the event of a natural disaster or a location-specific failure. JungleWP uses third-party monitoring services to track availability, with engineers on call to address any outages.

JungleWP is setup to operate from geographically distributed locations. By leveraging cloud resources, JungleWP infrastructure and customer support teams can support your business at any time.

Conclusion

We take security seriously at JungleWP. Customers using our service expect their data to be secure and confidential. Safeguarding this data is a critical responsibility we have, and we work hard to maintain that trust.

If after reading this whitepaper you have any further questions, please do not hesitate to contact our security team at support@junglewp.com.