Security Policy Document for Smoke With Me

Prepared for: Application Hosting & Infrastructure Review
Date: 30th July, 2025

1. Overview

This document outlines the current and planned security policies and protocols for our cloud-hosted application. The policies aim to demonstrate a proactive and structured approach to securing data, infrastructure, and access management. This ensures compliance with modern security standards, instills confidence in stakeholders, and supports future scalability.

2. Current Hosting Infrastructure: Cloudways on DigitalOcean

Our application is currently hosted on Cloudways using DigitalOcean infrastructure. Cloudways provides a managed hosting solution with multiple layers of integrated security, powered by Imunify360.

2.1 Core Server-Level Security Features

All Cloudways servers come pre-equipped with the following protections:

- **Advanced Firewall:**
  - Protects against brute-force, port scanning, and DoS attacks.
  - Uses a cloud-based traffic analysis system to block malicious behavior.

- **Web Application Firewall (WAF):**
  - Inspects HTTP traffic to block SQL injections, XSS, and other OWASP Top 10 vulnerabilities.
  - Tailored for CMS platforms such as WordPress, Joomla, and Drupal.

- **Brute Force and Spam Protection:**
  - Monitors login activity across SSH, SFTP, and control panel.
  - Automatically blocks repetitive or suspicious attempts.

- **Weak Password Detection:**

    - Ensures accounts and access points are not vulnerable to dictionary attacks or compromised credentials.

- **Malware Protection (via Security Suite Add-on):**
    - Optional but enabled for comprehensive malware scanning, real-time threat prevention (RASP), and file/database/script inspections.

2.2 Account & Access Security

- **SSH/SFTP IP Whitelisting:**
    - SSH and SFTP connections are restricted to whitelisted IPs only. This prevents unauthorized access.

- **Two-Factor Authentication (2FA):**
    - Enabled for all Cloudways account access to ensure credential theft alone cannot grant unauthorized access.

3. Application-Level Security Controls

3.1 Securing Files from Direct Access

- All media and configuration files are stored outside the public web root wherever possible.
- .htaccess rules and/or middleware are used to restrict access to sensitive directories.
- Uploaded files are scanned via Imunify360 malware protection.
- Direct file access is protected using signed URLs or token-based access mechanisms.

3.2 Securing the Database

- Cloudways restricts direct database access via firewall rules and internal IP access only.
- Database access is protected using strong, encrypted passwords.
- Connections to the database are secured via SSL wherever supported.
- Access is only granted to necessary services (application backend and admin panel) on a least privilege basis.

3.3 Role-Based Access Control (RBAC)

- Each role is granted only the minimum permissions required to perform their responsibilities.
- Backend APIs and Admin dashboards enforce these roles via authentication and authorization middleware.

3.4 API Security with Auth Tokens

- All APIs use token-based authentication (e.g., JWT). Tokens are short-lived and transmitted over HTTPS.

4. Planned Infrastructure Migration to AWS

To support greater scalability and enterprise-grade security, we are planning a phased migration to Amazon Web Services (AWS).

4.1 AWS Security Advantages

- **Amazon EC2 with Security Groups & IAM:**
  - Granular control over traffic with security groups, allowing only essential ports/IPs. IAM roles and policies ensure access management with least privilege.

- **Amazon RDS:**
  - Secure, encrypted database instances with automatic backups, multi-AZ failover, and network isolation via VPC.

- **AWS Key Management Service (KMS):**
  - Enables encryption of sensitive data at rest using customer-managed keys.

- **AWS Shield & WAF:**
  - Advanced protection against DDoS and malicious web requests.

- **Amazon CloudWatch & GuardDuty:**
  - Continuous monitoring and threat detection for abnormal behavior and potential compromise.

- **S3 with Presigned URLs:**
  - File storage with private access and time-bound file sharing capabilities.

- **Serverless Architecture via AWS Lambda:**
  - Minimizes attack surface and allows execution of backend logic in isolated containers without maintaining long-lived servers.

5. Conclusion

With robust protections in place via Cloudways and a clear roadmap to AWS with industry grade security practices, our infrastructure and application are fully aligned with best practices for data protection, access control, and threat mitigation. This foundation ensures secure data storage, secure transmission, and reliable auditability critical to earning investor trust and ensuring long-term scalability.