PhishTACO

ZibaSec Security Overview

Introduction

ZibaSec’s mission is to reduce the human vulnerabilities in your organization across social attack vectors through training and simple defensive mechanisms.

We believe that an effective phishing simulation and defense platform should train and educate your people while building their trust in your security organization.

One of our most important responsibilities is to ensure the security of your data. We commit to transparency and helping you understand our approach.

Organizational Security

ZibaSec’s security program is something we take pride in and is based on defense-in-depth principles: we have a robust set of policies and technical controls that secure our company and your data at every layer. Our security program is aligned with NIST standards (we are FedRAMP In Process) and is constantly evolving with updated guidance and industry best practices. View details of our FedRAMP certification here.

While our Chief Technology Officer is responsible for the implementation and management of our security program, as a small team, we’ve implemented a culture of security-first development and innovation. Every member of our engineering team actively contributes to application and infrastructure security, security engineering, incident response, and risk and compliance.

All of our employees undergo a comprehensive 7-year background check and are US persons (due to Federal requirements).

Protecting Customer Data

Our primary security objective is the protection of our customer data. To this end, our team has, in partnership with industry partners, taken steps to identify and mitigate risks, implement best practices, and work in a state of continuous improvement.

Secure By Design

We've built and designed a robust software development lifecycle that leverages a high degree of automation and multiple checks for every change and every deployment. You can read about how we leverage our partner GitHub for static code analysis, change-control, and production access on the official Github Blog.

Encryption

- **In transit:** All communication channels are encrypted via TLS 1.2 including all database-related operations. Where possible, all transport channels leverage FIPS-compliant endpoints and encryption algorithms. **Note**: We send emails as part of phishing campaigns via optimistic TLS.
- **At rest:** We keep all data encrypted at rest using FIPS validated encryption which is backed by AWS KMS.

Perimeter and Runtime Security

PhishTACO's perimeter is protected by AWS WAF and AWS Shield to mitigate against a variety of common attack scenarios to include DDoS and injection attacks. ZibaSec personnel access all systems through the use of FIPS validated hardware tokens and must use a VPN to access privileged parts of the application.

Our AWS environment and databases are constantly scanned and monitored for adherence to CIS benchmarks which are further augmented by our engineering team.

At runtime, each customer interaction with PhishTACO is backed by a short-lived AWS Lambda function. Each individual interaction (eg click) triggers a unique Lambda container that only processes the data of the given user, and nobody else. Our Lambda containers typically run for less than 1 second and are incapable of executing for more than 30 seconds which significantly reduces the surface of attack in our infrastructure.

Access Control

- **Provisioning**
  We adhere to the principles of least privilege and role-based permissions when provisioning access—employees are only authorized to access data that they reasonably must handle in order to fulfill their current job responsibilities. All production access is reviewed at least quarterly.
- **Authentication**
  To further reduce the risk of unauthorized access to data, ZibaSec employs hardware-based multi-factor authentication for all access to systems, including our production environment, which houses our customer data. Where possible and

appropriate, ZibaSec uses private keys for authentication, in addition to the previously mentioned multi-factor authentication on a physical token.

- **Password Management**
  ZibaSec requires personnel to use an approved password manager. Password managers generate, store, and enter unique and complex passwords to avoid password reuse, phishing, and other password-related risks.

System Monitoring, Logging, and Alerting

ZibaSec monitors all services (AWS, etc) to retain and analyze a comprehensive view of the security state of its infrastructure. Administrative access, use of privileged commands, and system calls on all components in ZibaSec's production network are logged and retained for at least two years. Analysis of logs is automated to the extent practical to detect potential issues and alert responsible personnel. All production logs are stored in an isolated environment that is restricted to only the relevant personnel.

Data retention and disposal

Customer data is removed immediately upon deletion by the end-user or as requested by the customer administrator. ZibaSec hard deletes all information from currently-running production systems and backups are destroyed within 45 days. ZibaSec's hosting providers are responsible for ensuring the removal of data from disks is performed in a responsible manner before they are repurposed.

Disaster Recovery and Business Continuity Plan

ZibaSec utilizes services deployed by AWS to distribute production operations across multiple physical locations. These locations are within one US-based geographic region, but protect ZibaSec's service from loss of connectivity, power infrastructure, and other common location-specific failures. Production transactions are replicated among these discrete operating environments to protect the availability of ZibaSec's service in the event of a location-specific catastrophic event. ZibaSec also retains a full backup copy of production data in a remote (US) location significantly distant from the location of the primary operating environment. Full backups are saved to this remote location at least once per day and transactions are saved continuously. ZibaSec tests backups at least quarterly to ensure they can be successfully restored.

Responding to Security Incidents

ZibaSec has established policies and procedures for responding to potential security incidents. All security incidents are managed by ZibaSec's security team. The policies and procedures define the types of events that must be managed via the incident response process and classifies them based on severity. In the event of an incident, affected customers will be informed via email from our executive team. Incident response procedures are tested and updated at least annually.

Vendor Management

To run efficiently, ZibaSec relies on sub-service organizations. Where those sub-service organizations may impact the security of ZibaSec's production environment, we take appropriate steps to ensure our security posture is maintained by establishing agreements that require service organizations to adhere to confidentiality commitments we have made to users. ZibaSec monitors the effective operation of the organization's safeguards by conducting reviews of all service organizations' controls before use and at least annually.

Sub Service organizations currently include:

- Google Workspaces
- AWS
- ZenDesk
- SumoLogic
- Slack
- GitHub

External Validation

- **Security Compliance**
  ZibaSec is continuously monitoring, auditing, and improving the design and operating effectiveness of our security controls. These activities are regularly performed by both third-party credentialed assessors and our engineering team. Audit results are shared with senior management and all findings are tracked to resolution in a timely manner.
- **Penetration Testing**
  In addition to our compliance audits, ZibaSec engages independent entities to conduct application-level and infrastructure-level penetration tests at least annually. Results of these tests are shared with senior management and are triaged, prioritized, and remediated in a timely manner. Customers may receive executive summaries of these activities by requesting them from support.
- **Customer Driven Audits and Penetration Tests**
  Our customers are welcomed to perform either security controls assessments or penetration testing on ZibaSec's environment. Please contact support to learn about options for scheduling either of these activities.

Conclusion

We have an existential interest in protecting your data. Every person, team, and organization deserves and expects their data to be secure and confidential. Safeguarding this data is a critical responsibility we have to our customers, and we continue to work hard to maintain that trust. Please contact us if you have any questions or concerns.