QuestionPro

QUESTIONPRO SECURITY OVERVIEW

At QuestionPro, the security of customer data is a top priority. QuestionPro is committed to the confidentiality, integrity, and availability of all information within its system. The staff at QuestionPro work daily to fortify each of its security policies, procedures, and controls to meet the most demanding information security standards in the US and worldwide.

PHYSICAL SECURITY

Data Center: QuestionPro owned and managed servers are co-located in an Internap data center and are backed up in separate facility at the Azure data center. QuestionPro restricts physical access to the data centers to senior personnel on a least privilege basis. The data centers are monitored twenty-four hours a day, seven days a week. Visitors to the center are logged and escorted throughout the facility by data center personnel. All visitors must wear ID badges. The centers utilize security guards, electronic access devices, biometric access devices, fire alarm systems, and CCTV monitoring.

Data Center Compliance: Internap, QuestionPro’s primary data center, undergoes periodic SSAE 16 SOC 2 audits. Reports from these audits confirm Internap’s commitment to protecting against unauthorized access and to maintaining constant data availability. QuestionPro’s backup facility, Azure undergoes periodic SSAE 16 SOC 2 audits. Reports from both these facilities are available for review upon request.

ACCESS AND AUTHENTICATION

Customer User Authentication:

Single Sign-On: Single Sign-on (SSO) allows QuestionPro users to access with the credentials of an existing company intranet. SAML, multipass/token, or cookie based SSO can be used with popular authentication systems, such as Active directory or LDAP, to determine if an end-user is authenticated.

Double Opt-in Verification and reCaptcha: QuestionPro offers the ability for customers to require reCaptcha verification upon user registration. reCaptcha helps prevent automated scripts from creating fake accounts.

Email Based Access Restrictions: The QuestionPro Academic license allows university customers to limit registrations to individuals with email address domains of the university.

QuestionPro Personnel Authentication: Any access to QuestionPro servers (including production environment, staging environment, and databases) requires multi-factor authentication—SSH keys and passphrases. Access to the staging environment is limited to developers; access to the production environment is limited to system administrators; and access to the databases is limited to senior system administrators.

ADMINISTRATIVE SECURITY

Least Privilege: QuestionPro employs the concept of least privilege—qualified employees are allowed access to privileged areas of the system only when such access is necessary for the operation of QuestionPro business functions. Privileged accounts are only granted to appropriately qualified employees in order for them to perform essential duties.

Account Management: QuestionPro employee accounts may not be created or modified without the approval of a Senior System Administrator. Each account holder is allocated an individual username and password. Employees must notify a Senior System Administrator when moving to a

new position or location within QuestionPro. In order to ensure appropriate access, a Senior System Administrator must alter a moving staff member's access privileges according to his or her new responsibilities. The Senior System Administrator must make these alterations immediately upon being notified. Directly thereafter, the Senior System Administrator must communicate the changes made to the appropriate QuestionPro personnel.
Management is also responsible for notifying a Senior System Administrator of any staff changes.

Username and Password Security: Logon passwords must never be written down or disclosed. All passwords must be at least 8 characters in length. A combination of lower case letters, capital letters, numbers, and special characters must be used. Easily guessed passwords must not be used. Account holders must change their passwords every ninety days. Any logged-in user will be automatically timed out of his or her account after fifteen minutes of inactivity. All unused usernames are automatically disabled after six months of inactivity. QuestionPro staff must never permit another individual to utilize their username to access the QuestionPro network. The owner of a particular username will be held responsible for all actions performed using this username.

For additional information regarding administrative security and the regulation of access to the QuestionPro system, please refer to QuestionPro Access Control Policy.

SYSTEM MONITORING

QuestionPro utilizes monitoring tools such as Nagios, CloudFlare, and OSSEC in conjunction with the logging capabilities of Apache Logs, Linux var/log/audit/audit.log, and MySQL Statistics to generate audit records and to monitor the QuestionPro system twenty-four hours a day. With these tools, System Administrators can select specific events to audit at each layer of the system, including internal system access, failed authentication attempts, and other auditable events. Additionally, these tools allow for the time stamping of all auditable actions and enable the creation of audit trails to support after-the-fact investigations of security incidents.

BOUNDARY SECURITY

Firewall: All external connections to the QuestionPro system terminate on an iptables/Linux firewall configured with a default “deny all” rule. Uninitiated outbound traffic is limited to external APIs (translation services, etc.) and SMTP. The firewall utilizes non-standard managed access points for HTTP traffic, SSL encrypted HTTP traffic, and SMTP outbound traffic.

Additional Boundary Protection: QuestionPro utilizes IP blacklists to lock out IP addresses that are known to be fraudulent, the integrity checker OSSEC to detect whether any unauthorized changes to the system have occurred, and the boundary protection service CloudFlare to create logical boundaries and to defend against DDoS attacks.

VULNERABILITY SCANS

QuestionPro performs periodic vulnerability scans of the QuestionPro system. All discovered vulnerabilities are given an immediate security risk assessment and addressed in accordance with the assessment determination. PCI security reports are available for review upon request.

CONFIGURATION/RELEASE MANAGEMENT

QuestionPro follows a release and maintenance methodology that includes the documenting, testing, and review of proposed changes to the system. QuestionPro updates its server operating systems with the latest patches on a timely basis and issues maintenance releases at least weekly. All non-essential applications are disabled to protect the system from internet-based threats.

DEVELOPMENT PRACTICES

As part of its development process, QuestionPro maintains separate environments for development, staging, testing, and production in accordance with SDLC best practices. Access to the production environment is limited to system administrators. All development code is reviewed by a senior admin before into production. QuestionPro protects against SQL injections through prepared statements, stored procedures, escaping user-supplied input, and enforcing least privilege.

QuestionPro combats cross-site scripting by using proper escaping/encoding, blacklists, vulnerability scans, and other procedures.

ENCRYPTION

Data in Transit: QuestionPro implements SSL, TLS, SSH, and SCP encryption to securely transfer data. QuestionPro supports full SSL encryption, and all mail servers are configured with TLS. Access to system servers is only allowed via SSH on a non- standard port. Data is transferred to the backup data center via SSH using rsync.

Data at Rest: QuestionPro hash encrypts all customer passwords and credit card data stored within the system databases. When customers use SSO, passwords are not stored but are authenticated with a token.

DATA PRIVACY

Separation of Data: All customer data, including the data of end users, is logically separated by account-based rules that require the entry of a unique username and password with each logon.

Employee Regulations: Prior to hiring, QuestionPro employees and contractors are subjected to criminal background screening and notified that any improper sharing of customer or Community Member data will result in the loss of employment. All employees and contractors must sign non-disclosure agreements upon joining the company.

Additional Privacy Details: See the QuestionPro Privacy Policy for additional details at https://www.questionpro.com/help/1.html and https://www.questionpro.com/security/

COMPLIANCE

International Compliance: QuestionPro coplies with the US-EU Safe Harbor Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries. In compliance with these frameworks, QuestionPro adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement, and commits to resolve complaints about privacy and the collection or use of personal information. Additionally, QuestionPro has further committed to refer unresolved privacy complaints under the US-EU Safe Harbor Principles to an independent dispute resolution mechanism operated by the Council of Better Business Bureaus. QuestionPro is constantly reviewing, developing, and fortifying its security controls, policies, and procedures to meet the compliance demands of its U.S. agency clients.

Additional Compliance: QuestionPro is Section 508 compliant, a BBB accredited business, and its privacy policy is TRUSTe certified--one of the most respected privacy certifications available.
See QuestionPro Compliance for additional details at
https://www.questionpro.com/compliance/

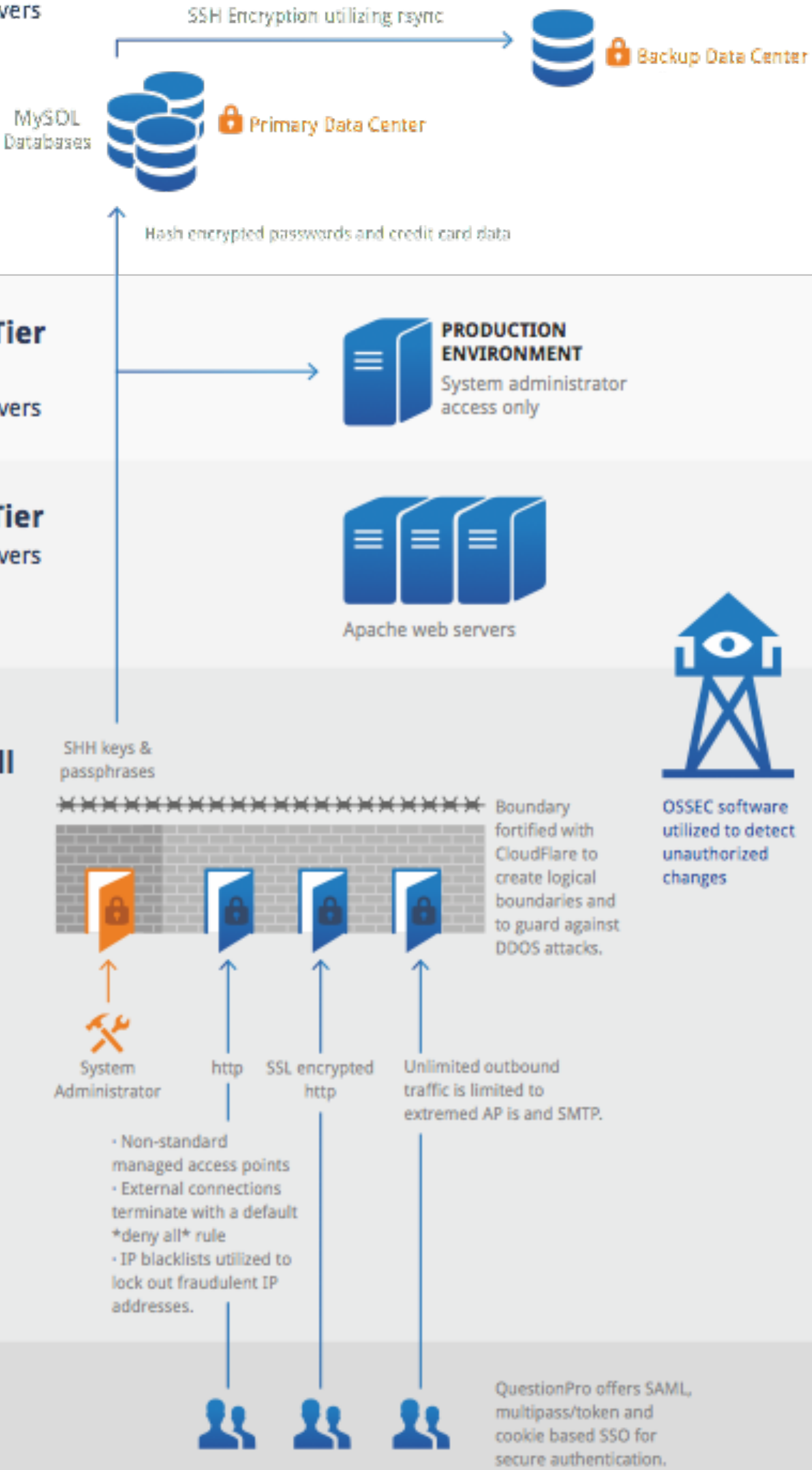
AVAILABILITY

Backup: QuestionPro executes continuous hot backups that are available for restore within two hours. Only system administrators have access to the backups and only for the purpose of a system restore. Under no circumstances will backups be removed from the servers.

Uninterruptible Power Supply: All QuestionPro servers are outfitted with uninterruptible power supply (UPS) units to provide instant emergency power in the case of a power failure.

Support: QuestionPro offers twenty-four hour email and chat support five days a week. Additionally, clients have unlimited access to an online knowledge base with over five hundred help articles, screenshots, and videos at https://www.questionpro.com/help/

Business Continuity, Incident Response, and Disaster Recovery: QuestionPro has implemented policies and procedures to manage any actual or potential crisis or security incident that threatens QuestionPro operations or customer data.



Data Tier

Linux CentOs Servers

SSH Encryption utilizing rsync

MySQL Databases

Primary Data Center

Backup Data Center

Hash encrypted passwords and credit card data

Application Tier

Resin J2EE

Linux CentOs Servers

PRODUCTION ENVIRONMENT

System administrator access only

Web Server Tier

Linux CentOs Servers

Apache web servers

iptables/ Linux firewall

SHH keys & passphrases

Boundary fortified with CloudFlare to create logical boundaries and to guard against DDOS attacks.

OSSEC software utilized to detect unauthorized changes

System Administrator

http

SSL encrypted http

Unlimited outbound traffic is limited to extremed AP is and SMTP.

- Non-standard managed access points
- External connections terminate with a default *deny all* rule
- IP blacklists utilized to lock out fraudulent IP addresses.

QuestionPro Clients

(End users)

QuestionPro offers SAML, multipass/token and cookie based SSO for secure authentication.