SurveyGizmo Security White Paper

Version: 2.2

June 2, 2016

This document is being given to you to help you understand the security environment and culture of SurveyGizmo, and to answer questions that you may have from your security team.

This document may be used in place of traditional security assessment checklists to help you with your due diligence. Possession of this document falls within SurveyGizmo's Terms of Use.

Our team strives to ensure accurate information, but because we are always evolving our security posture to match current and changing conditions, this document may not always reflect our exact architecture and it may not be error free.

Where we reference Amazon/AWS, some of these sections were pulled directly from Amazon's security white paper.

We reserve the right to modify this information at any time.

Questions or comments: compliance@surveygizmo.com

Table of Contents

Executive Summary

At SurveyGizmo we take data security very seriously.

SurveyGizmo is an exceptionally powerful, easy to use software that gives you access to the answers you're after, no matter your budget. Collect data of all kinds on our global, scalable, reliable platform, then use our reporting tools to find trends and patterns.

Because SurveyGizmo is primarily a Do-it-Yourself (DIY) application and is utilized globally, we strive to ensure compliance with specific requirements, but we don't guarantee it. We have implemented a holistic and comprehensive approach to both security and privacy, but SurveyGizmo does not claim to have a complete understanding of all the unique compliance and privacy requirements for each country. See the SurveyGizmo Privacy Whitepaper for more information on compliance.

We give you the tools, but it is up to you to implement them correctly. Ultimately, the security of the data you collect is your responsibility.

Your data is protected with numerous anti-hacking measures, redundant firewalls, and constant security scans. Because security is so important to us, our CEO has approved all Information Security and Privacy policies, and our Team Directors and Managers are responsible for compliance and security at the team level.

In addition to undergoing full background checks, all employees attend security awareness and compliance training when they start at SurveyGizmo. There is also an annual refresher training for current employees.

Finally, we annually review all our Security and Privacy policies, and this SurveyGizmo Security Document is frequently updated to bring you up-to-the-moment information about our data protection efforts.

Some of our most important security initiatives include:

- All of our software and services are online, and we don't require any software downloads.
- We offer multiple methods for survey taking, such as web browsing, offline mode, QR codes, smartphones, and tablets.
- Through Amazon Web Services (AWS), we have a fault-tolerant, highly available (HA), and scalable infrastructure. We employ redundant firewalls and load balancers to protect against intrusion and surges in traffic volume. We are committed to providing a 99.9% uptime for survey takers and application users, and in 2015 we were able to provide 99.95% availability.

Environment

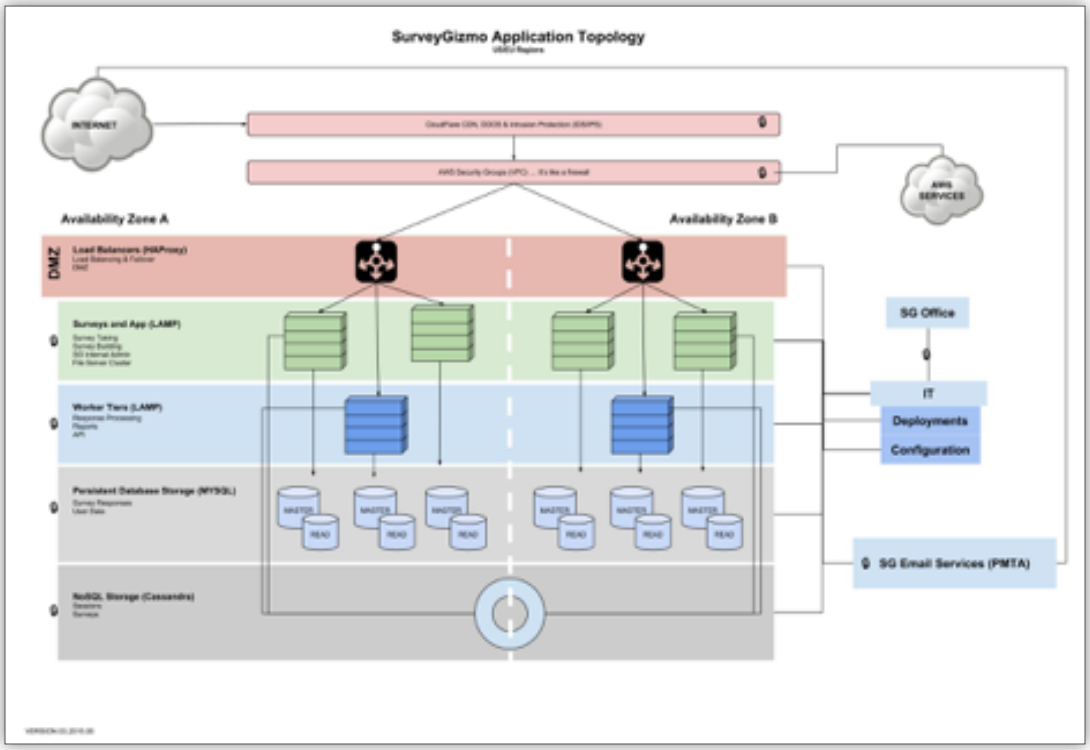
We are located in Boulder, Colorado, and we utilize AWS for our hosting services.

We have separate development, test, and production environments for both our website and application. Work progresses from development to quality assurance to production, where it can be seen and used by our customers.

A modified Lean Agile Systems Development Life Cycle (SDLC) methodology is used for development, and issues are reported from both clients and employees. Issues are tested and documented in Support and prioritized by the Product Development Team.

Production servers are only accessed through Secure Shell (SSH), or from the office network through a Virtual Private Network (VPN).

Robust monitoring software is used to monitor performance and notify us of any problems in our production environment. The checks include, but are not limited to, business logic, database layer, disk space, resources, and application logs.



Third-Party Architecture

Because we are hosted by AWS, we leverage their power to be highly available, to increase our reliability, and to offer increased flexibility that lets us scale up for surges in traffic in almost real-time.

Automated redundancies are in place for a scalable infrastructure to accommodate high traffic. Because of this, security in the cloud is slightly different than security in on-premise data centers.

We have a shared security responsibility model with AWS. We utilize AWS for Infrastructure as a Service (IaaS), and they are responsible for the underlying infrastructure that supports the cloud. They are responsible for protecting the global infrastructure that runs all of the services offered in the AWS cloud. This infrastructure is comprised of the hardware, software, networking, and facilities that run AWS services.

For more information on Amazon's extensive security controls, see their Overview on Security Paper.

AWS is also responsible for the security configuration of their products that are considered managed services. These services provide the scalability and flexibility of cloud-based resources with the additional benefit of being managed.

For these services, AWS will handle basic security tasks like guest operating system (OS) and database patching, firewall configuration, and disaster recovery.

In the US, we are part of the US East (VA) Region, which has 5 highly redundant and reliable zones. They are located in New York, NY; 2 in Dallas TX; 2 in Ashburn, VA.

In the EU, our datacenter is located in Frankfurt, Germany, which is part of the EU Central region.

For security reasons and as part of AWS policy, AWS doesn't provide the physical addresses of the data centers. The main reason our customers would want the physical address is to ensure the data centers are sufficiently geographically separated to conform to standard disaster recovery requirements. AWS ensures they have that level of redundancy and reliability, which eliminates the need for actual physical addresses.

Physical Security

According to the AWS Security whitepaper, AWS data centers are state of the art, utilizing innovative architectural and engineering approaches.

Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure.

AWS data centers are housed in nondescript facilities. Physical access is strictly controlled, both at the perimeter and at building ingress points by professional security staff, utilizing 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.

All physical access to data centers by AWS employees is logged and audited routinely.

Endpoint Management

We use industry standard endpoint protection software on all company laptops. Laptop scanning is scheduled to run daily, and employees are encouraged to report any errors to the privileged IT Admins. We manage administrator privileges on all equipment and all new laptops are encrypted.

Coding Practices

To ensure a secure platform, we utilize the Open Web Application Security Project (OWASP) standards during the software development process. We focus on not only improving the functionality of our product, but on also improving the security of our software.

All members of the Product Development Group are required to adhere to the OWASP top 10 standards: injection; weak authentication and session management; cross-site scripting; insecure direct object references; security misconfiguration; sensitive data exposure; missing function level access control; cross-site request forgery; using components with known vulnerabilities; and unvalidated redirects and forwards. For more information please see: OWASP top 10.

We use a code repository along with a managed ticketing, review, and approval process. Our development team utilizes standard quality assurance procedures, and automated regression testing is performed prior to each production deployment.

We also never outsource; all development and quality assurance activities are performed in-house.

We never use production data for testing purposes, unless it is required to resolve a client-reported support issue.

Network Security Features

AWS Firewalls

According to the AWS Security white paper Amazon EC2 provides a complete firewall solution; this mandatory inbound firewall is configured in a default deny-all mode, and we explicitly open the ports needed to allow inbound traffic.

The traffic is restricted by protocol, by service port, and by source IP address (individual IP or Classless Inter-Domain Routing (CIDR) block).

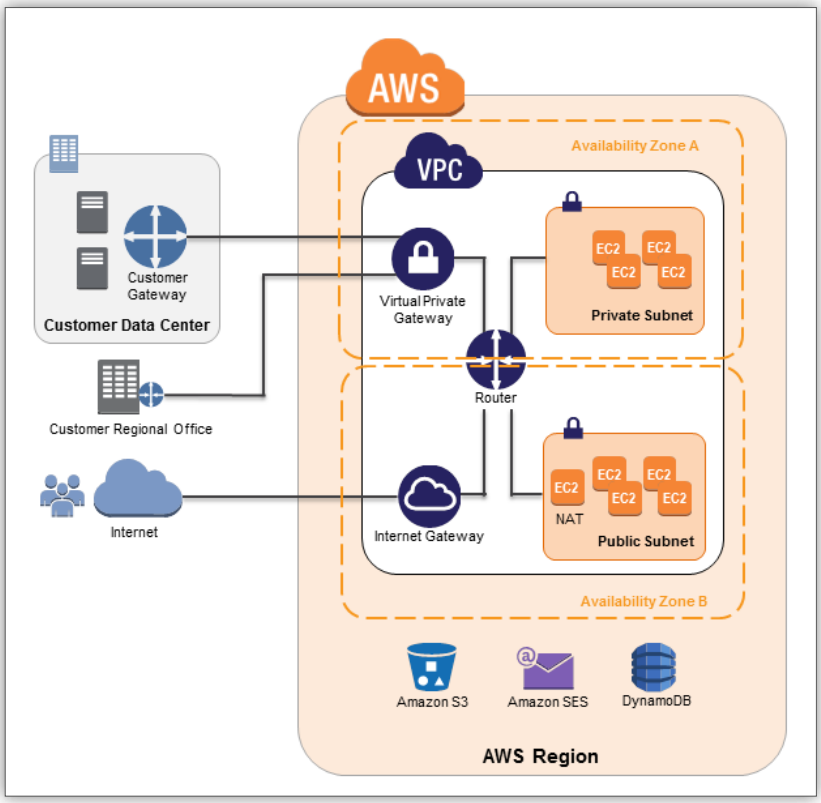


Figure 5: Amazon VPC Network Architecture

Amazon Web Services - Overview of Security Processes - August 2015 page 28

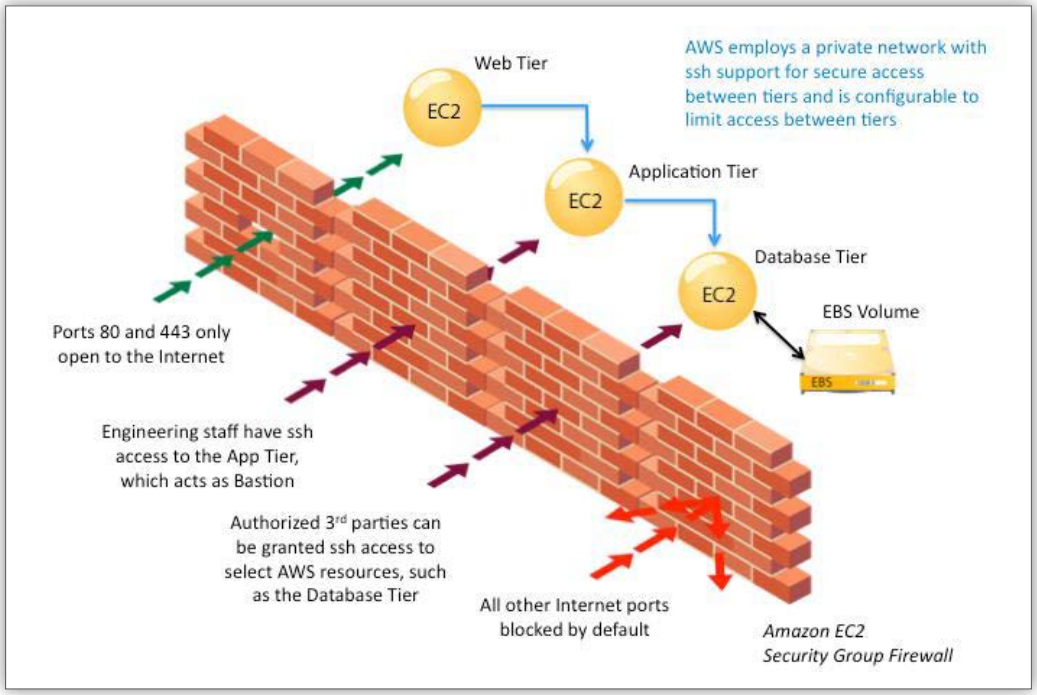


Figure 4: Amazon EC2 Security Group Firewall

Amazon Web Services - Overview of Security Processes - August 2015 page 23

The AWS firewall resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. All packets must pass through this layer, thus an instance's neighbors have no more access to that instance than any other host on the Internet. They can be treated as if they are on separate physical hosts.

The physical RAM is separated using similar mechanisms. The firewall isn't controlled through the guest OS; rather, it requires a X.509 certificate and key to authorize changes, adding an extra layer of security.

To eliminate IP Spoofing, the firewall will not permit an instance to send traffic with a source IP or MAC address other than its own.

AWS technologies: Web Application Firewall/CloudFront/Route 53.
Functions Include: IDS,IPS,blacklists, DDoS and spoofing prevention.
AWS technologies: Virtual Private Cloud/Security Groups/Network ACLs, EC2
Functions include: Subnet acls, inbound and outbound port restrictions, DMZ proxy layer.
Host-based protection: Functions include: subnet/port acls
Additional technologies: The DMZ proxy layer which includes software that provides additional layer 3-7 protection

AWS Secure Network Architecture

According to AWS security whitepaper network devices, including firewall and other boundary devices, are in place 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, are established on each managed interface, which manage and enforce the flow of traffic. ACL policies are approved by Amazon Information Security. These policies are automatically pushed using AWS's ACL Manage tool, to help ensure these managed interfaces enforce the most up-to-date ACLs.

AWS Secure Access Points

According to AWS security whitepaper they have strategically placed a limited number of access points to the cloud to allow for a more comprehensive monitoring of inbound and outbound communications and network traffic. These customer access points are called API endpoints, and they allow secure HTTP access (HTTPS). This access type allows you to establish a secure communication session with your storage or compute instances within AWS.

In addition, AWS has implemented network devices that are dedicated to managing interfacing communications with internet service providers (ISPs). AWS employs a redundant connection to more than one communication service at each internet-facing edge of the AWS network. These connections each have dedicated network devices.

Amazon Corporate Segregation

According to AWS security whitepaper logically, the AWS Production network is segregated from the Amazon Corporate network by means of a complex set of network security and segregation devices.

AWS developers and administrators on the corporate network who need to access AWS cloud components in order to maintain them must explicitly request access through the AWS ticketing system. All requests are reviewed and approved by the applicable service owner.

Approved AWS personnel then connect to the AWS network through a bastion host that restricts access to network devices and other cloud components, logging all activity for security review. Access to bastion hosts require SSH public key authentication for all user accounts on the host.

AWS Fault-Tolerant Design

According to AWS security whitepaper Amazon's infrastructure has a high level of availability and provides its customers with the capability to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal customer impact.

Data centers are built in clusters in various global regions. All data centers are online and serving 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.

Application Architecture

LAMP & N-Tier

SurveyGizmo is a traditional LAMP based application. LAMP is an acronym which stands for Linux operating system (OS), Apache HTTP Server, MySQL relational database management system (RDBMS), and PHP programming language.

We've developed SurveyGizmo as an N-Tier Application using the MVC (Model-View-Controller) Design pattern.

The multi-tier (N-Tier) architecture is a client-server software architecture platform in which the presentation (web application), the processing/function logic (workers), and the database are logically separated processes.

This allows any part of the three tiers to be developed and maintained independently of the others, creating maximum flexibility and the ability to respond to technology changes in any one tier.

MVC is a software architecture pattern for implementing user interfaces on computers. These architectural decisions help to create separate of the different logical responsibilities of the application.

Application Scalability & Redundancy

In order to support scaling and redundancy of the SurveyGizmo platform, we utilize the following solutions:

Federated Multi-tenant Database Designs

In order to ensure that data collected for different purposes can be processed separately, SurveyGizmo logically separates the data of each of its clients.

We ensure that each customer has a unique login ID, and that data segmentation is keyed off a unique customer ID. Each customer has a unique user name (email address) and a unique password.

After repeated, unsuccessful logins, the lockout features prevent the login page from being resubmitted. By federating our data, we are also able to scale horizontally to support increasing users and customers.

Background Queued Processes

We leverage a number of queuing systems to defer jobs that do not need to be transactional. This allows us to scale up and down the number of queues and workers to mirror the demands on our systems without impacting the front-end experience of users in the application.

Redundant Data Stores

To ensure that we never lose any of our customer's data, we have multiple strategies utilizing redundant data stores. This includes, but not limited to RAID-based storage, write / read Databases, and in-memory caching.

Application Security Features

Data Encryption

All survey data, even those that are designated as unencrypted, are encrypted at the disk level on the database servers. Surveys that are designated by the customer as encrypted are further encrypted at the row level.

Our redundant databases reside in a private subnet that is only accessible via our application and web servers. Additionally, we leverage Amazon's AWS security features to further "lock down" access to these systems. Bulk response data can only be accessed via the reporting and exporting features available via the application by a customer logging in with their credentials over HTTPS.

When surveys are flagged to be encrypted (by the customer), we further encrypt the data at the row level when it's inserted into the database on those drives. The Project Data Encryption feature allows you to encrypt stored data or data "at rest."

This means that stored data cannot be accessed without a key, and therefore provides a higher level of protection for your stored data. Project Data Encryption must be activated on a survey-by-survey basis. Once you have collected data in an encrypted survey, encryption cannot be enabled/disabled.

Access to the SurveyGizmo Application is available only through secure HTTPS. Data in transit is encrypted when customers choose to use HTTPS protocols for their account, API, or survey. We utilize TLS for our secure communication protocol and we are currently at the most recent patch level.

Additionally, data is encrypted at rest and additional layers of encryption can be enabled, managed, and controlled via a client-facing feature.

Encryption is generally used by companies that collect sensitive information such as ePHI (personal health information), but it can be used for anyone who wants to keep their stored data protected.

We provide 256-bit encryption for all data. This is extremely secure, and is used by health care companies and the military to secure their data. All backups in our system utilize 256-bit encryption as well.

Secure Survey Share Links

If you wish to take advantage of an extra layer of security when collecting data, you can use secure links, designated by the HTTPS protocol. HTTPS links use a Secure Socket Layer (SSL) to transport data safely between client and survey using an encryption algorithm.

Password Settings

Some SurveyGizmo customers collect highly sensitive data that requires the utmost security, while others find these stringent measures annoying.

Passwords are stored using a salted encryption. Application credentials - username/passwords are NEVER logged. If you choose to use the login/password action, this information is stored in clear text so this shouldn't be used for sensitive data collection. SurveyGizmo personnel will not reset user passwords. In the event of a password being misplaced, users are sent a unique link via email, which they will use to reset their password.

To accommodate our wide range of users, our password security settings allow administrators to determine the precise level of security necessary to protect each SurveyGizmo account.

An administrator can configure these options within their account:

- **Expiration Interval:** Set a time interval for password expiration (e.g. 3 days to 12 months)
- **Password Reuse Rules:** Disallow password reuse, either by password history or interval of time elapsed (e.g. every X passwords or every X months/years)
- **Minimum/Maximum Length:** Specify a minimum and/or maximum password length
- **Require at least one upper and one lowercase letter:** Choosing this option requires all users' passwords to contain at least one uppercase and one lowercase letter
- **Require at least one number:** Choosing this option requires all users' passwords to contain at least one number
- **Require at least one special character:** Choosing this option requires all users' passwords to contain at least one special character
- **Set up a complex rule (using Regex):** You can specify your own password pattern using Regular Expressions (Regex)
- **Password cannot contain SurveyGizmo user information:** This makes it impossible for users to incorporate their username, email address, or user id into their password.

Scanning and Patching

Firewall logs and other logs are restricted to authorized users via secure multi-factor authentication (MFA) controls. We utilize Amazon's Recommend MFA, and only our privileged IT Admins have access to this information.

Local systems are protected with industry standard antivirus software.

Production servers are Linux-based and frequently patched to ensure their security is always up to date. Security patches are applied within 2-3 days of notification of the patches being available. We roll patches out through the development rollout process outlined earlier in this document: development to QA to production.

When vulnerabilities are identified, our mitigation scale is as follows:

- Critical: addressed immediately
- High: addressed within 72 hours
- Medium: included in the next appropriate sprint

We utilize Burp Suite to perform a passive quarterly internal scan, and we use McAfee to perform a weekly third party external scan. The results of these tests are not publically available. For the period of April 2016 - March 2017, we utilize WhiteHat Security to do an annual penetration test on SurveyGizmo; their report is at the end of this document.

Logging and Alerting

We utilize intrusion detection (IDS) and Intrusion Prevention (IPS)PS at multiple layers of the application, with extensive logging and alerting capabilities. We monitor criteria for thousands of different alerts ranging from customer experience and application health to server and service metrics. Logs are kept for a minimum of 60 days are are stored in AWS.

We maintain user access log entries that contain the date, time, customer information, operation performed, and source IP address. If there is suspicion of inappropriate use, SurveyGizmo can provide customer log entry records to assist in forensic analysis. This service is provided on a time and materials basis.

Disaster Recovery

We have a disaster recovery plan that includes shared responsibilities with Amazon and it is reviewed annually. Amazon utilizes disaster recovery facilities that are geographically remote from their primary data center. When using AWS disaster recovery shared security model, they provide the physical infrastructure, network, and operating systems, and SurveyGizmo ensures the proper configuration and logical access to the resources.

Reliability and Backup

All network components are configured in a redundant configuration. All customer data is stored on a primary database server with multiple active clusters for redundancy. The database servers utilize RAID disks and multiple data paths to ensure reliability and performance.

Automated encrypted snapshots (differentials) of databases are performed daily, and all data storage is redundant. Encrypted daily snapshots are maintained for a minimum 30 days and test restores are conducted at least quarterly.

Backup media resides on AWS' Simple Storage Service (S3) infrastructure, which offers '11 9s' of redundancy.

Data Retention

SurveyGizmo retains data that we process on behalf of our customers and data collected directly from our customers as long as it is needed to provide services to our customers. SurveyGizmo will retain and use this data as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements. Sometimes users have unique needs, either under specific regulations or other institutional or state requirements, that require exceptions to these guidelines. If you need your data deleted, you are responsible to contact SurveyGizmo and request this action.

For instance, occasionally data needs to be completely destroyed after its intended use. In many cases, data is retired and locked away rather than actually destroyed (e.g. when a customer stops paying for an account, downgrades to a different account plan, etc.).

In most cases this makes the loss retrievable in the event of a mistake. We can, however, comply with a request for total data destruction if necessary.

Incident Response Plan

Incident Response is a significant aspect of any Information Technology program. Preventive activities such as application scanning, password management, intrusion detection and intrusion prevention systems, firewalls, risk assessments, malware & anti-virus prevention, and user awareness and training can reduce the number of incidents; however, not all incidents can be prevented.

Incident Response capabilities are necessary for detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring services.

Our plan covers the Incident Response Requirements, Roles and Responsibilities of each Incident Response Team member, their contact information, Incidents Handling Procedures, Incident Reporting Procedures, and complementary metrics.

We have procedures for normal business hours as well as for after-hours and weekends. All employees are trained in the procedures, and they understand how and when to escalate an issue.

Our Compliance Manager and the IT Manager are responsible for enforcing information security policies, procedures, and control techniques to address all applicable requirements. They also ensure 100% participation of personnel in the Security Awareness Training Program.

Our Incident Response Team consists of the Director of Operations, Director of Development, Compliance Manager, IT Manager, and specific IT administrative and support staff.

Breach Notification

Suspected incidents are reported to the Team Managers, who are responsible for organizing the investigation and notifying internal stakeholders. If the investigation finds a need for containment, that will occur, then analysis will follow. If repair, recovery, or remediation is needed, that will follow.

Notifications to clients will be made based on contractual or legal obligations, reporting will be made to Executive Management, and training issues will be addressed. If a breach is detected with your data, you will be notified as soon as we are able.

Security Standards

In 2016, we are implementing the CIS Critical Security Controls. We utilize the NIST Special Publication 800-53 Revision 4 series as a reference for all policy documents. We perform a risk assessment and self audit, which is done each fall. All employees receive annual refresher Security Awareness Training.
We do not allow unauthorized, external parties to conduct testing against our systems. It is our policy that we do not share, at any level, the policies and procedures related to the security and compliance of our systems.

Security Skills Assessment and Appropriate Training

Policies

All employees are required to sign a Non-disclosure Agreement (NDA), Mobile Request Agreement, Bring Your Own Device (BYOD), and a Work from Home (WFH) Policy.

Bring Your Own Device (BYOD)

All employees are issued company-owned equipment, and all company-owned equipment is managed by the office IT administrators. Per company policy, employees cannot access customer data from their personal devices, including laptops and cellphones.

Training

We have developed a robust, ongoing training plan for all new and existing employees. All new employees are required to attend seven days of SurveyGizmo training.

During this training, in addition to the application training they also attend the following:

- two-hour Welcome and Orientation
- two-hour SG Brand and Lifecycle of an SG Customer
- three-hour Giving Great Service
- one-hour Security and Compliance Training session

In 2016, we implemented user behavior training during which we 'phish' our own employees. This training allows us to train our employees on good email and web browsing habits.

We utilize a method of assessing their knowledge and identifying areas of vulnerability, educate and perform quick lessons learned, followed by additional training if needed. We are constantly measuring and reinforcing good internet-use habits.

Existing employees receive annual refresher Security Awareness Training. We have a weekly company meeting where the Executive Management Team reports our revenue, expenses, and account numbers. We also utilize this time with the entire company to discuss important topics, like security and compliance training.

Our 2016 Security and Compliance Training Initiatives are as follows:

- Q1 - Physical Security
- Q2 - Incident Handling
- Q3 - Privileged Access
- Q4 - Compliance and Risk Management

Background Checks

We partner with an employment screening vendor to complete background checks on all employees before they are hired. The human resources department completes reference checks on all employees. We comply with the federally mandated requirements regarding I-9 (The Employment Eligibility Verification Form) documentation.

WhiteHat Web Application Attestation

May 2016

Whitehat Security
Web Application Security Attestation

SurveyGizmo commissioned WhiteHat Security to perform technical Web Application Security assessments on its web applications to evaluate the security controls. WhiteHat Security performs ongoing security assessments to derive actionable security data, including description of Internet threats, vulnerabilities, and application coding weaknesses. This data is provided to SurveyGizmo via the Sentinel Portal, reporting, and the Sentinel API. All of these data sources are available 24/7.

As part of the Sentinel Premium Edition Service, WhiteHat Security conducts both automated and Business Logic testing. Automated testing utilizes Sentinel, an automated vulnerability scanner, that provides continual web security assessment testing of web applications with an easy to use web portal and application programming interface (API). This service combines automated assessment for technical vulnerabilities with custom testing performed by the WhiteHat Security Operations Team to manually identify business logic flaws. This provides continuous application assessments. All vulnerabilities are verified for accuracy by the WhiteHat operations team to ensure accurate and actionable results. This service provides SurveyGizmo with an up-to-date status of web application vulnerabilities on any given day.

WhiteHat Security simulates the activities of external attackers that may present a threat to SurveyGizmo's Web applications by utilizing:

1. Unauthenticated testing - A user who does not have access to the web application.
2. Authenticated testing - A malicious authorized user, or an unauthorized user who has compromised an account.

WhiteHat Security's vulnerability management scanners are updated regularly with new vulnerability threats. This feature is designed to address new vulnerabilities as they are discovered; reducing the time a web application is at risk of exploitation.

The Sentinel DAST service levels (Premium, Standard, and Pre-Launch) tests for the following list of WASC 2.0 classes of Web vulnerabilities, as defined at http://projects.webappsec.org/w/page/13246978/Threat%20Classification . The Sentinel Source vulnerability classes are defined as WASC 2.0 vulnerability classes, as well as a set of vulnerability classes per programming language and framework.

Ryan O'Leary, Sr. Director TRC

Stripe PCI Attestation of Compliance

Attestation of Compliance, SAQ A, Version 3.1

Section 1: Assessment Information

Part 1. Merchant and Qualified Security Assessor Information

Part 1a. Merchant Organization Information

Company Name: SurveyGizmo
DBA(s): WWW.SURVEYGIZMO.COM
Contact Name: Christian Vanek
Title: Company Representative
Email: michelle@sgizmo.com
Telephone: 8006096480
Business Address: 4888 Pearl East Circle, Suite 100W
City: Boulder
State: CO
Zip: 80301
Country: US
URL: www.surveygizmo.com
Part 1b. Qualified Security Assessor Company Information (if applicable)
N/A

Part 2. Executive Summary

Part 2a. Type of Merchant Business (check all that apply)

[ ] Retailer
[ ] Telecommunication
[ ] Grocery and Supermarkets
[ ] Petroleum
[x] E-Commerce
[ ] Mail order/telephone order (MOTO)
[ ] Others

What types of payment channels does your business serve?
[ ] Mail order/telephone order (MOTO)
[x] E-Commerce
[ ] Card-present (face-to-face)

Which payment channels are covered by this SAQ?
[ ] Mail order/telephone order (MOTO)
[x] E-Commerce
[ ] Card-present (face-to-face)

Part 2b. Description of Payment Card Business

How and in what capacity does your business store, process and/or transmit cardholder data?
We do not store, process and/or transmit cardholder data

Part 2c. Locations

N/A

Part 2d. Payment Application

Does the organization use one or more Payment Applications? NO
Provide the following information regarding the Payment Applications your organization uses: N/A

Part 2e. Description of Environment

Provide a high-level description of the environment covered by this assessment:

Our customers dispatch all cardholder data securely to Stripe, our payments processor, via an iframe. Our company's servers receive an opaque token object, from which the original cardholder data cannot be derived.
Does your business use network segmentation to affect the scope of your PCI DSS environment? YES

Part 2f. Third-Party Service Providers

Does your company share cardholder data with any third-party service providers (for example, gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)? YES

Name of service provider: Stripe, Inc.

Description of services provided: Collection, storage and processing of all cardholder data.

Part 2g. Eligibility to Complete SAQ A

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because:

YES - Merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions);

YES - All processing of cardholder data is entirely outsourced to PCI DSS validated third-party service providers;

YES - Merchant does not electronically store, process, or transmit any cardholder data on merchant systems or premises, but relies entirely on a third party(s) to handle all these functions;

YES - Merchant has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and

YES - Merchant retains only paper reports or receipts with cardholder data, and these documents are not received electronically.

YES - For e-commerce channels, all elements of the payment page or pages delivered to the consumer's browser originate only and directly from a PCI DSS validated third-party service provider.

Section 2: Self-Assessment Questionnaire A

9.5: Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)? Media refers to all paper and electronic media containing cardholder data. N/A

9.6: Is strict control maintained over the internal or external distribution of any kind of media? Controls should include the following: N/A

9.6.1: Is media classified so the sensitivity of the data can be determined? N/A

9.6.2: Is media sent by secured courier or other delivery method that can be accurately tracked? N/A

9.6.3: Is management approval obtained prior to moving the media (especially when media is distributed to individuals)? N/A

9.7: Is strict control maintained over the storage and accessibility of media? N/A

9.8: Is all media destroyed when it is no longer needed for business or legal reasons? Media destruction should be performed as follows: N/A

9.8.1: (a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed? (b) Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents? N/A

12.8: Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows: YES

12.8.1: Is a list of service providers maintained? YES

12.8.2: Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment? YES

12.8.3: Is there an established process for engaging service providers, including proper due diligence prior to engagement? YES

12.8.4: Is a program maintained to monitor service providers PCI DSS compliance status at least annually? YES

12.8.5: Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity? YES

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

Based on the results noted in the SAQ A dated 2016-03-25, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document as of 2016-03-25:

YES - Compliant: All sections of the PCI SAQ are complete, and all questions answered yes, resulting in an overall COMPLIANT rating, thereby SurveyGizmo has demonstrated full compliance with the PCI DSS.

NO - Non-Compliant: Not all sections of the PCI DSS SAQ are complete, or not all questions are answered affirmatively, resulting in an overall NON-COMPLIANT rating, thereby SurveyGizmo has not demonstrated full compliance with the PCI DSS. Target Date for Compliance: An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. Check with your acquirer or the payment brand(s) before completing Part 4.

NO - Compliant but with Legal exception. One or more requirements are marked NO due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.

Part 3a. Acknowledgement of Status

YES - This PCI DSS Self-Assessment Questionnaire, Version 3.1, was completed according to the instructions therein.

YES - All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.

YES - I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.

YES - I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.

YES - If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

YES - No evidence of full track data1, CAV2, CVC2, CID, or CVV2 data2, or PIN data3 storage after transaction authorization was found on ANY system reviewed during this assessment.

N/A - ASV scans are being completed by the PCI SSC Approved Scanning Vendor (ASV Name).

Part 3b. Merchant Attestation

Signature of Merchant Executive Officer: Christian Vanek

Date: 2016-03-25

Merchant Executive Officer Name: Christian Vanek

Title: Company Representative

Merchant Company Represented: SurveyGizmo

Part 3c. QSA Acknowledgement (if applicable)

N/A

Part 3d. ISA Acknowledgement (if applicable)

N/A

Part 4. Action Plan for Non-Compliant Requirements

N/A

Appendix C: Explanation of Non-Applicability

Requirement: 9.X Reason Requirement is Not Applicable: No part of our environment, including any type of media, transmits, stores or processes cardholder data. As such, there is no cardholder data to restrict access to.

AWS Service Organization Controls (SOC) 3 Report

Here is the link to AWS's report. This report is dated 4-25-16 and is relevant to security and availability for the period of October 1, 2015 - March 31, 2016.

References

This document was created with the following references:
https://aws.amazon.com/compliance/resources/
https://aws.amazon.com/security/
https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf
https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf