Security White Paper

Version 3.0

Last Updated: December 2017

Date: December 19, 2017

Confidential - do not duplicate or distribute without written permission from SurveyGizmo. This is a controlled document that can only be obtained from the SurveyGizmo portal, which requires that you provide your name and contact details.

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.

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

SurveyGizmo's offices are located at 4888 East Pearl Circle in Boulder, Colorado. It is an energetic and dynamic place to work which allows employees the freedom to express themselves while working very hard to provide the best services and application to the customers. A few remote offices are located in the United States and employees are allowed to work from home. The Boulder offices are accessed via secure badge access only and there is a strict visitor policy.

SurveyGizmo is a midsized business so the definition of "formal" and "documented" is whether the process is predictable and constantly repeatable. SurveyGizmo has implemented the exact level of policies, standards, plans, and procedures for the environment. SurveyGizmo follows similar guidelines as bigger companies and how these guidelines are implemented aligns with the corporate vision and mission.

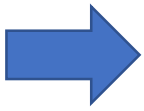
SurveyGizmo has a lean agile development environment with bi-weekly sprints. Release are sometime done multiple times per day. These releases are automatic and the customer does not decide if and when they are applied. SurveyGizmo may from time to time, in its sole discretion, change some or all of the functionality or any component of the SurveyGizmo application.

Applications with customer specific information are only available while employees are physically in the Boulder office or through a VPN connected to the physical office. By policy, SurveyGizmo does not allow employees to work from "Starbucks like" locations or use a split-tunnel VPN. SurveyGizmo has multiple employee policies including an Acceptable Use policy. New Hire training is mandatory and SurveyGizmo provides quarterly training updates.

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.

Because SurveyGizmo is hosted by AWS, SurveyGizmo leverages their power to be highly available, to increase the reliability, and to offer increased flexibility that lets SurveyGizmo scale up for surges in traffic in near real time. 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 the services offered in the AWS cloud. This infrastructure is comprised of the hardware, software, networking, and facilities that run AWS services.

Unlike the traditional on premise software model, where the customer has 100% responsibility for securing their systems. When a customer utilizes a Cloud Service Provider (CSP), they are now utilizing the shared security model. AWS has a model which can be found in the Shared Responsibility Model. Below is the SurveyGizmo shared security model. Depending on the CSP model either Infrastructure-as-a-Service (Iaas), Platform-as-a-Service (PaaS), or Software-as-a-Service (SaaS) selected, the level of responsibility shifts from one part to the other. In all the models, White indicates the Customer's Responsibility; the Light Grey is AWS's Responsibility; and the Dark Gray is SurveyGizmo's Responsibility.

Customer 

Shared Security Diagram		
IaaS	PaaS	SaaS
Physical	Physical	Physical
Infrastructure	Infrastructure	Infrastructure
Network	Network	Network
Virtualization	Virtualization	Virtualization
Operating System	Operating System	Operating System
Application	Application	Application
Service Configuration	Service Configuration	Service Configuration
Access	Access	Access
Data	Data	Data

For more information on Amazon's extensive security controls, see their Overview on Security Paper or checkout their enormous library of resources.

Application & Interface Security

Application Development

SurveyGizmo is a traditional Linux, Apache, MySQL, and PHP (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 a multi-tier (N-Tier) Application using the MVC (Model-View-Controller) Design pattern.

The 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.

We also never outsource; all development and quality assurance activities are performed in-house. The SurveyGizmo application is 100% developed by employees.

- We use supported 3rd party libraries as necessary to enhance and produce new features.
- Manual Source Code review before check-in.
- Peer Review for critical code.
- State Code Analysis tool.
- We use Jenkins for automated DevOps.

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

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 System 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). VPN is IPSEC and traffic is logged.

Audit Assurance

Independent Audits

Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.

SurveyGizmo utilizes WhiteHat Security https://www.whitehatsec.com/ to perform an annual application penetration test on the SurveyGizmo application. SurveyGizmo also utilizes the WhiteHat Security application scanner to do continuous scanning of the application.

SurveyGizmo utilizes TrustWave https://www.trustwave.com/home/ to perform quarter network penetration tests on the SurveyGizmo network environment.

SurveyGizmo staff also utilizes Burp Suite https://portswigger.net/burp to perform their own quarter scans.

SurveyGizmo hired an independent, third-party to perform a Health Insurance Portability and Accountability Act (HIPAA) audit.

Customers Auditing SurveyGizmo

We don't allow customers to perform application or network penetration testing on us.

Security Incident Management

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 to notify.

Business Continuity Management & Operational Resilience

The purpose of preparing for contingencies and disasters is to provide for the continuation of critical missions and business functions in the event of disruptions. SurveyGizmo has both a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP). The BCP refers to strategies about how the business should plan for both interruptions in service and continuation after a disaster. The BCP allows for the advance planning to ensure the business has defined its critical business products and services and that these critical assets can continue to be delivered. While the DRP refers to how the information technology and information systems should recover in the event of a disaster. The DRP should detail what should be done immediately after a disaster to recover from the event.

Service Health and Failover

Customers can subscribe to the SurveyGizmo Status IO page for immediate notification of issues related to the SurveyGizmo application. https://surveygizmo.statuspage.io/ As the SurveyGizmo application is completely reliant on the availability of AWS, customers can customize the following AWS page for their availability. http://status.aws.amazon.com/ Also, if you send emails via the SurveyGizmo application, you can ensure that RackSpace (the hosting provider for email service) is available via the following page. https://rackspace.service-now.com/system_status/. We currently don't allow our customers to move away from either AWS or RackSpace as the hosting provider.

Business Continuity Plan (BCP)

The BCP identifies the critical business functions needed to ensure the availability of essential services and programs and ensures the continuity of operations. The identification of critical business functions is called a Business Impact Analysis (BIA). Continuity planning is one component of a much broader

emergency preparedness process that includes items such as contingency planning, business practices, and operational continuity. Preparing for such events often involves implementing policies and processes at an organizational level and may require numerous plans to properly prepare for, respond to, recover from, and continue activities if impacted by an event. Managers must also consider the impacts of disruptions and plan, in alignment with organizational standards and policies, for such events. As one component of a comprehensive risk management approach, Business Continuity planning should identify potential vulnerabilities and threats and then implement approaches to either prevent such events from happening or limit their potential impact.

SurveyGizmo's BCP identifies the types of incidents which could lead to the activation of the BCP and it includes the roles and responsibilities of SurveyGizmo staff should the plan be activated. To help with ranking of tasks, it includes a BIA which was developed by determining the business processes and recovery criticality, identifying resource requirements, and then identifying recovery priorities for system resources.

Disaster Recovery Plan (DRP)

By definition, a disaster cannot be prevented but steps can be taken to eliminate or reduce the impact of the disaster on the business. For SurveyGizmo, a disaster could be complete loss of AWS Availability Zones for more than 24 hours, compromise of information/architecture integrity for more than 24 hours, natural disaster that destroys Boulder Offices, or global to local environmental factors. A great deal of consideration is taken to ensure that if a disaster occurs the necessary strategies are in place to reduce the impact to our customers. Some of the preventive measures that SurveyGizmo utilizes are ensuring proper support for data migration and durable storage from AWS, ensuring proper alerting, ensuring good backups, ensuring employees have connections from their homes, and monitoring early warning systems.

The DRP identifies the requirements to recover the information technology assets from a disaster. It also defines the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) and Maximum Tolerable Downtime (MTD). Organizations whose major applications are processed at a shared facility should work with the facility management to develop a plan for post-disaster recovery (i.e., which applications/buildings/systems should be restored first). SurveyGizmo has a DRP 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.

The following recovery plan objectives have been established for SurveyGizmo:

- Identify the activities, resources, and procedures to carry out SurveyGizmo processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated personnel and provide guidance for recovering SurveyGizmo during prolonged periods of interruption to normal operations.
- Coordinate Disaster Recovery planning activities with Business Continuity actions and Incident Response activities.
- Ensure coordination with external points of contact and vendors associated with SurveyGizmo.
- Ensure coordination with other plans associated with SurveyGizmo.

Plan Testing

Test and exercise events should be conducted periodically to determine the plan's effectiveness and to ensure that all personnel know their role and are informed of the specific actions required of them. For each test and/or exercise activity which is conducted the results will be documented and lessons learned action items will be taken so that the associated plans, polices, and procedures can be updated. We annually test the BCP and DRP.

Business Impact Analysis (BIA)

As stated above, to help with ranking of tasks, our BCP includes a BIA which was developed by determining the business processes and recovery criticality, identifying resource requirements, and then identifying recovery priorities for system 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 hourly, 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. You can go to this location for more information on deletion. https://help.surveygizmo.com/help/delete-data

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.

Change Control & Configuration Management

System modifications can introduce risks to system integrity or reliability as well as threats to data confidentiality unless the systems include adequate controls. Change management is the process of requesting, analyzing, approving, developing, implementing, and reviewing a planned or unplanned change within the IT infrastructure. The change management process begins with the creation of a change request within SurveyGizmo's selected technology platform. It ends with the satisfactory implementation of the change and the communication of the result of that change to all interested parties.

The system risk impact from changes and the risk probability of adverse events falls into three categories:

- Low - If an adverse event is encountered, the financial damage or confidential data exposure is minimal or non-existent. The risk of an adverse event is statistically very low and would require prevention measures that outweigh the expenditure of resources (both time or money) to gain a significant improvement in order not to encounter this risk.
- Medium - If an adverse event is encountered, the financial damage or confidential data exposure impact is moderate, and could be outside of the risk tolerance for SurveyGizmo. The risk of an adverse event is statistically moderate and the investment of resources to mitigate the possibility of an event would essentially cost about as much as the impact of the event in resources.
- High - If an adverse event is encountered, the financial damage could be high, the financial damage or exposure of confidential data could be widespread or critical. The risk of an adverse event is statistically high. The adverse effects far outweigh the investment in resources to significantly reduce the likelihood of an event or to reduce the overall risk impact of damages to place it into a lower Risk Impact category.

In addition to impact and probability, the scope or number of components touched during a change also can partially determine the security risk. In general, more places touched means the potential for more risk. SurveyGizmo defines scope as small, medium, large, and extra-large with extra-large being the riskiness.

Data Security & Info Lifecycle

We allow the ability for customers to permanently delete their data from our systems. Due to being a multi-tenant solution, backups for any individual tenant will be permanently deleted once the age of the backup exceed the age of the oldest backup being retained.

Datacenter Security

According to the AWS Security whitepaper, AWS's 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. In the US, we are part of the US East (VA) Region, which has 5 highly redundant and reliable zones. They are in New York, NY; DA3 & DA6, Dallas TX; DC6 & DC10 Ashburn, VA. In the EU, our datacenter is 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.

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

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.

Encryption & Key Management

Data encryption is a primary control to protect confidential information from unauthorized access or misuse. Privacy laws in some US states designate data encryption as the only control that can help avert claims for negligence in protecting confidential information, and provides safe harbor from being required to disclose a data breach.

SurveyGizmo employees do not on a regular basis transmit protected confidential information. SurveyGizmo employees do not store confidential information in clear text on their laptops, smart phones or other mobile devices.

AWS Encryption of Data at Rest

All data at rest is encrypted on disk using AWS EBS encrypted volumes. AWS provides the ability to encrypt EBS volumes and their snapshots with AES-256. The encryption occurs on the servers that host the EC2 instances, providing encryption of data as it moves between EC2 instances and EBS storage.

Encryption Methodology and Key Strength

All encryption is accomplished using non-proprietary industry standard encryption algorithms. Where possible, SurveyGizmo will ensure that strong encryption keys are implemented. AES-256 key length and greater are recommended encryption algorithms and key strengths.

Encryption Key Management

Encryption keys whether created and managed by SurveyGizmo or an encryption solution vendor, are securely stored and maintained.

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. 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, via survey specific application level encryption. This means that stored data cannot be accessed without a key and algorithm that is managed outside of the data store, 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 client-facing features.

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. By default, all newly created standard web links are secured by default.

Governance & Risk Management

The SurveyGizmo IT Risk Management Program integrates risk identification and mitigation with policy and regulatory IT compliance management. SurveyGizmo will implement and maintain an IT Risk Management Program that will leverage industry best practices, guidelines and standards, and include the following elements.
SurveyGizmo will:

- Perform an IT Risk Assessment and analysis at least once per year.
- Develop and implement Policies and Standards to meet IT risk mitigation objectives as well as maintaining compliance with privacy and other regulatory requirements.
- Establish a remediation prioritization process that allocates a priority level to the threat and vulnerabilities that have the potential to cause significant impact or harm to SurveyGizmo services, systems, devices, or confidential data.
- Perform an information technology risk assessment and select adequate controls to mitigate known risks. The controls will be consolidated in a Risk Register. An IT Risk Assessment will be performed prior to deployment of new or modified systems.

Risk Determination is used to assess the level of risk to the IT systems. The determination of risk for a particular threat/vulnerability pair will be measured using a risk level matrix. The risk level matrix will be expressed in terms of probability and impact level as shown below:

Security Standards

In 2016, we are implementing the CIS Critical Security Controls. We also utilize the Open Web Application Security Project (OWASP) standards during the software development process. 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.

Human Resources

The purpose of implementing a Human Resources Standard is to ensure that data and IT Assets are used in an appropriate, responsible, and legally compliant manner consistent with the business strategy of SurveyGizmo. The Human Resource Standard ensures the confidentiality, integrity, and availability of SurveyGizmo systems and data. The following describes how our employees are managed.

- All employees are subject to background verification.
- We specifically train our employees in regard to their specific role and information security controls they must fulfill.
- All employee training is documented with their acknowledgement of completion.
- All personnel are required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer information.
- All personnel are trained and provided with security awareness training programs at least once a year.
- We have documented policies, procedures and guidelines in place to govern change in employment and/or termination. Our documented policies, procedures and guidelines account for timely revocation of access and return of assets.
- We can provide documentation regarding how we may access customer data via an Acceptable Use Policy.
- Users are made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements and understand the sanctions for non-compliance.
- Users are made aware of their responsibilities for leaving unattended equipment in a secure manner.
- 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.

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.

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.

Security Skills Assessment and Appropriate Training

Security Training and measurement is the responsibly of the Security and Compliance Manager. The 9th annual, Verizon 2016 Data Breach Investigation Report (DBIR) states that the human threat vector is the most pressing issues today. Our employees are our biggest weakness and that 63% of confirmed

breaches involved weak, default, or stolen passwords. To combat this threat, SurveyGizmo ensures management support, increases employee awareness of security issues, measures our success, and continuously improves our methods. Studies show that it takes 90 days to break a habit and 90 days to form a new habit so a successful program will take consistent attention and determination to turn our employees from security liabilities to security assets.

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

Phishing

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.

Access Provisioning Management

Access will be provisioned to users based on specific job on a *'need to know'* basis. Users will be provided the least amount of access required to successfully complete their job requirements. A request to provision access to systems or data beyond those normally required for job responsibilities that include administrative access or elevated access to confidential data must be reviewed and approved by SurveyGizmo Senior Management.

Administrative Access

Administrative privileges must be limited to only those administrator accounts required to manage or maintain systems, applications or data**.** Only Administrator accounts will be used to perform administrative functions. All other user accounts will have lower levels of privilege. High level system privileges such as 'root', administrator, *SA* or default user file permissions that allow unrestricted access to computer systems are reserved for IT system administration.

Access for Third Party IT Solution and Service Provider

SurveyGizmo utilizes AWS, a third-party provider of IT solutions and services, to provide the SaaS services including network and system infrastructure to support SurveyGizmo IT needs. AWS has agreed to

maintain the confidentiality, integrity and availability of the systems and data per their IT Security Policies, and contractual obligations to SurveyGizmo.

- A contract was entered into with AWS in July 2014. The standard terms of use were utilized with no customization.
- A Business Associate Agreement (BAA) was signed with AWS on June 10, 2015.
- A Data Processing Agreement (DPA) was signed with AWS on September 20, 2016.

SurveyGizmo utilizes Salesforce, for customer support ticketing.

- A contract was entered with Saleforce in 2016. The standard terms of use were utilized with no customization.
- A Business Associate Agreement (BAA) was signed with Salesforce on January 23, 2017.
- A Data Processing Agreement (DPA) was signed with Salesforce on December 14, 2016.

Password Settings

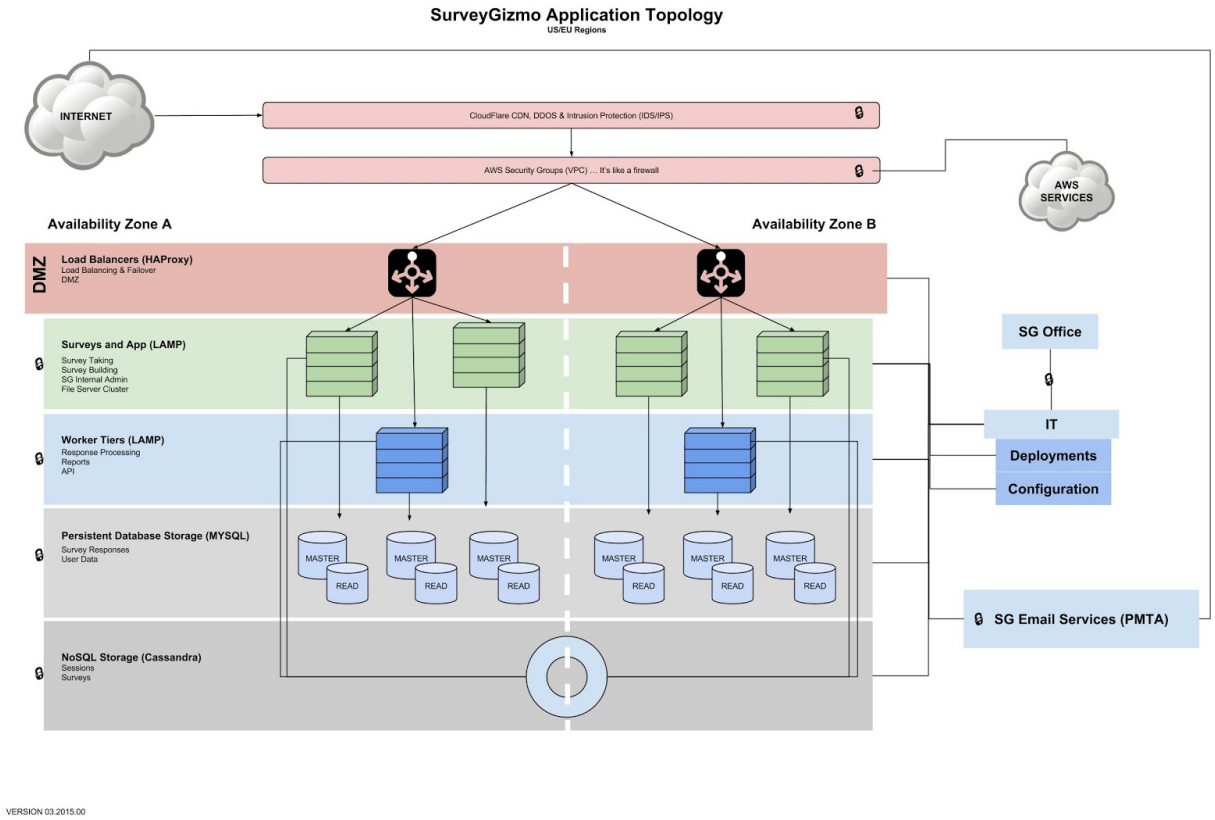
Passwords are stored using a salted encryption. Application credentials - username/passwords are NEVER logged. If you choose to use the login/password action, this information is stored in clear text so this shouldn't be used for sensitive data collection. SurveyGizmo personnel will not reset user passwords.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

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

AWS Host Datacenter

The following is a high level view of SurveyGizmo's topology.



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).

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

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.

Additional technologies: The DMZ proxy layer which includes software that provides additional layer 3-7 protection
Host-based protection: Functions include: subnet/port acls

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

AWS Secure Network Architecture

According to the AWS Security White Paper, 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 the AWS Security White Paper, 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 the AWS Security White Paper, 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 the AWS Security White Paper, 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.

Logging & Alerting

The lack of effective system logging and monitoring reduces SurveyGizmo's ability to identify threats, cyber-attacks or security events.

Logs

Logs are kept for a minimum of 90 days and 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 suspicious of inappropriate use, SurveyGizmo can provide customer log entry records to assist in analysis. This service is provided on a time and materials basis.

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.

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 RAID-based storage, Master / Read Databases in-memory caching

Supply Chain Management

SurveyGizmo will identify, classify and fulfill the required business need through a concise and consistent Vendor Management process. SurveyGizmo prospective and current vendors will adhere to the same level of security that SurveyGizmo has.

SurveyGizmo requires the vendor procurement process to follow a specific set of steps before a determination is made to contract with a vendor for a particular business need. Creating and following an appropriate selection process, selection criteria and assignment of vendor risk level provides the consistency needed to ensure that all contracted vendors are fulfilling the required business need.

Threat & Vulnerability Management

Vulnerability management is a pro-active approach to managing network security. It includes processes for checking for and identifying vulnerabilities, verifying and mitigating vulnerabilities, and patching vulnerabilities. A vulnerability management program provides a way to assess, monitor and remediate vulnerabilities to IT Systems. Managing vulnerabilities helps to decrease the risk and exposure time that vulnerabilities can be exploited. Patches will also be deployed to minimize vulnerabilities resulting from non-patched systems.

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

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