Using Virtual Sprout Cloud Services - Common Privacy & Data Protection Considerations

Virtual Sprout

December 17, 2018

Overview

This document provides information to assist customers who use Virtual Sprout to store or process content containing personal data, in the context of common privacy and data protection considerations. It will help customers understand:

- The way Virtual Sprout services operate including how customers can address security
- The geographic locations where customers can choose to store content and other relevant considerations
- The respective roles the customer and Virtual Sprout each play in managing and securing content stored on Virtual Sprout services

Scope

This document focuses on typical Virtual Sprout customer concerns that arise while managing privacy and data protection requirements relevant to their business and use of Virtual Sprout services to store or process content containing personal data. A customer may need to comply with industry specific requirements, other jurisdictions where that customer conducts business, or contractual commitments a customer makes to a third party. These items are not within the scope of this document.

This document is provided solely for informational purposes. It is not legal advice and should not be relied on as legal advice. Each customer's requirements will differ. Customers should obtain appropriate advice on their implementation of privacy and data protection requirements, applicability of various Virtual Sprout services, and other requirements relevant to their business. When this document discusses content, it is referring to software (including virtual machine images), data, text, audio, video, images and other content that a customer, or any end user, stores or processes using Virtual Sprout services. A customer's content may include files and databases stored on a Virtual Sprout Cloud Disk. Such content may, but will not necessarily, include personal data relating to that customer, its end users, or third parties. The terms of the Virtual Sprout Master Services Agreement, Virtual Sprout Cloud Services Addendum, Virtual Sprout Acceptable Use Policy, or any other relevant agreement with Virtual Sprout governing the use of Virtual Sprout services apply to customer content. Customer content does not include data that a customer provides to Virtual Sprout in connection with the creation or administration of its Virtual Sprout accounts, such as a customer's names, phone numbers, email addresses and billing information – this is defined as account information and it is governed by the Virtual Sprout Privacy Statement located here: http://www.virtualsprout.com/privacy-policy/.

Customer Content: Considerations relevant to privacy and data protection

Storage of content presents all organizations with a number of common practical matters to consider, including:

- Will the content be secure?
- Where will content be stored?

- Who will have access to content?
- What regulations apply to the content and what is needed to comply?

These considerations are not cloud-specific and are relevant to internally hosted and operated systems as well as traditional third party hosted services. Each Virtual Sprout customer maintains ownership and control of their content in Virtual Sprout services, including control over:

- What content they choose to store or process using Virtual Sprout services
- Which Virtual Sprout services they use with their content
- The geographic location where their content is stored
- The format, structure and security of their content, including whether it is masked, anonymized or encrypted
- Who has access to their Virtual Sprout accounts and content and how those access rights are granted, managed and revoked

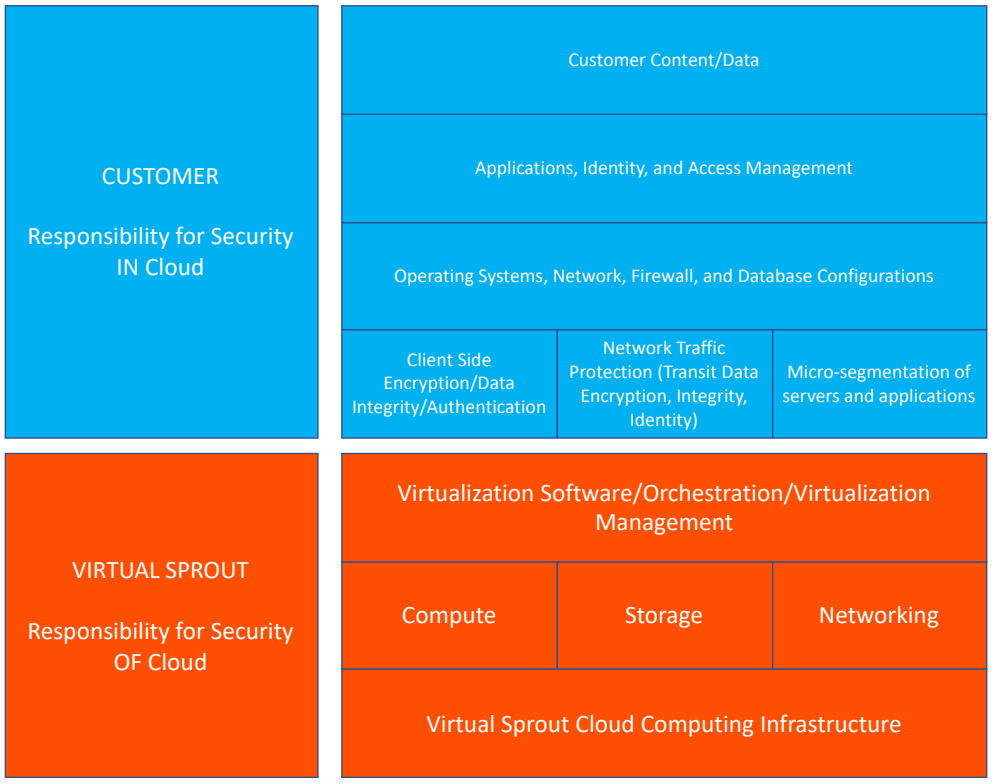
Because Virtual Sprout customers retain ownership and control over their content within the Virtual Sprout environment, they also retain responsibilities relating to the security of that content as part of the Virtual Sprout "shared responsibility" model.

Virtual Sprout Shared Responsibility Model

Customer Content Security

Content stored in Virtual Sprout services follows a shared responsibility model between the customer and Virtual Sprout. Virtual Sprout operates, manages and controls components from the host operating system and virtualization layer down to the physical security of the facilities in which the Virtual Sprout services operate. The customer is responsible for management of the guest operating system (including updates and security patches to the guest operating system) and associated application software, as well as the configuration of Virtual Sprout provided firewalls and other security-related features. Customers may connect to the Virtual Sprout environment through services the customer acquires from third parties or Virtual Sprout (for example, the Internet or private line connectivity such as E-Line or E-LAN services). These connections should be treated as non-trusted and the security of the content traveling over these connections is the customer's responsibility. Customers should consider the security of these connections and the security responsibilities of such third parties in relation to their systems. The roles of the customer and Virtual Sprout in the shared responsibility model are shown below:

SHARED RESPONSIBILITY DIAGRAM



How Does the Shared Responsibility Model Impact Security of Customer Content

Customers need to understand the differences between:

- Security measures that the service provider (Virtual Sprout) implements and manages – "security of the cloud/services"
- Security measures that the customer implements and operates, related to the security of customer content and applications that make use of Virtual Sprout services – "security in the cloud".

While Virtual Sprout manages security of the cloud, security in the cloud is the responsibility of the customer, as customers control what security they implement to protect their content, applications, systems, and networks – no different than if that content resided on-premise.

Understanding Security OF the Virtual Sprout Cloud Services

Virtual Sprout is responsible for managing the security of the underlying Virtual Sprout Cloud Services environment. Virtual Sprout utilizes highly secure data centers, electronic surveillance, and multi-factor access control systems. Data center access is authorized strictly on a least privileged basis. Additionally, all Virtual Sprout Cloud Infrastructure is segmented into secure locking cabinets accessible only to applicable Virtual Sprout technical staff.

Virtual Sprout Cloud Disk services provide encryption at rest for storing customer data, further protecting against risk of theft of physical storage medium. The Cloud Disk service dynamically re-keys at periodic intervals and upon the addition or removal of any storage media.

Virtual Sprout maintains a segmented management infrastructure, separate and apart from any customer services, compute, storage, and virtualization infrastructure. This infrastructure is protected by Virtual Sprout managed advanced perimeter firewalling, Intelligent Endpoint Detection and Response software, and other security measures. This infrastructure and related virtual systems are managed and monitored 24/7, 365 days a year by Virtual Sprout technicians.

Patching is a critical component to good security. All underlying hardware, software, virtualization platforms, and security components are patched on a best practices basis to provide both proper operation and optimal security.

Understanding Security IN the Virtual Sprout Cloud Services

Customers retain ownership and control of their content when using Virtual Sprout services. Customers, rather than Virtual Sprout, determine what content they store or process using Virtual Sprout services. The customer solely determines what level of security is appropriate for the content they store and process using Virtual Sprout. Customers have complete control over the services they use and whom they empower to access their content and services, including what credentials will be required. Customers control configuration of their environments and secure their content. This includes selective data encryption, data transit encryption, other security features and tools the customer chooses to deploy, and those tool's configurations. Virtual Sprout does not change or manage customer configuration settings, as these settings are determined and controlled by the customer. Virtual Sprout customers control their security architecture to meet their compliance needs. Virtual Sprout provides a wide selection of security tools and features customers can use. Customers can also use their own security tools and controls, including compatible third-party security solutions. Customers should always implement

- Strong password policies
- Assigning appropriate permissions to users
- Taking measures to protect access keys
- Firewalls and network segmentation
- Selective encryption of content
- Backup, Logging and DR services whether from Virtual Sprout or third-parties

Customers retain responsibility for their choices, and for security of the content they store or process using Virtual Sprout services including guest operating systems, applications on their virtual server instances, and content stored and processed in Virtual Sprout Cloud Disk. To assist customers with integrating Virtual Sprout security controls into their existing control frameworks, and to help customers design and execute security assessments of their organization's use of Virtual Sprout services, Virtual Sprout has numerous professional services relating to security, governance, risk and compliance. Customers can security scan their cloud infrastructure provided those scans are limited to the customer's cloud services and do not violate the Virtual Sprout Acceptable Use Policy12.

Virtual Sprout Geographic Locations: Where will content be stored?

Virtual Sprout customers choose the geographic location(s) in which their content and servers will be located during the onboarding and sales process. Virtual Sprout only stores and processes each customers' content in the Virtual Sprout geographic location(s) that were chosen during provisioning and will not move customer content without the customer's consent, except as legally required. Virtual Sprout currently only provides Cloud Services within the continental United States.

Who can access customer content?

Customer control over content

Customers using Virtual Sprout maintain and do not release effective control over their content within the Virtual Sprout Cloud Services. Customers:

- Determine where their content will be located
- Control the format, structure and security of their content, including whether it is masked, anonymized, or encrypted
- Manage other access controls such as identity access management, permissions, and security credentials

Customers control the entire life-cycle of their content on Virtual Sprout services and manage their content in accordance with their own specific needs including content classification, access control, retention, and deletion.

Virtual Sprout access to customer content

Virtual Sprout makes available to each customer compute, storage, networking, or other services, as described in Virtual Sprout's websites, service orders, and agreements between a customer and Virtual Sprout. Customers have a number of options to encrypt their content when using the services, including using Virtual Sprout encryption features such as Virtual Sprout Cloud Disk Encryption at Rest, managing their own Virtual Data Center encryption keys, or using a third-party encryption mechanism of their own choice. Virtual Sprout does not access or use customer content without the customer's consent, except as legally required. Virtual Sprout never uses customer content or derives information from it for other purposes such as marketing or advertising.

Government rights of access

Customers should seek advice to understand the application of relevant rules and regulations to their business and operations. Relevant government bodies may have rights to issue requests for content under laws and regulations that apply to the customer. Typically, a government agency seeking access to the data of an entity will address any request for information directly to that entity rather than to Virtual Sprout.

Most countries have processes (including Mutual Legal Assistance Treaties) to enable the transfer of information to other countries in response to appropriate legal requests for information (e.g. relating to criminal acts). Some countries have data access laws which apply extraterritorially. One such example is the United States Patriot Act. The Patriot Act applies to

companies with an operation in the U.S., irrespective of where they are incorporated and/or operating globally and irrespective of whether the information is stored in the cloud, in an on-site data center, or in physical records.

Virtual Sprout policy on granting government access

Virtual Sprout does not disclose or move data in response to a request from the U.S. or other government unless legally required to do so in order to comply with a legally valid and binding order, such as a subpoena or a court order, or as is otherwise required by applicable law. Non-governmental or regulatory bodies may use recognized international processes, such as Mutual Legal Assistance Treaties with the U.S. government, to obtain valid and binding orders. Virtual Sprout's practice is to notify customers where practicable before disclosing their content so they can seek protection from disclosure, unless legally prohibited from doing so or there is clear indication of illegal conduct in connection with the use of Virtual Sprout services.

Privacy Breaches

Given that customers maintain control of their content when using Virtual Sprout, customers retain the responsibility to monitor their own environment for privacy breaches and to notify regulators and affected individuals as required under applicable law. Virtual Sprout does not have visibility of customer access keys, or knowledge of who is and who is not authorized to log into an account. Therefore, the customer is responsible for monitoring use, misuse, distribution or loss of credentials and customer access keys. In some jurisdictions it is mandatory to notify individuals or a regulator of unauthorized access to or disclosure of their personal data and there are circumstances in which notifying individuals will be the best approach in order to mitigate risk, even though it is not mandatory under the applicable law. It is for the customer to determine when it is appropriate or necessary for them to notify individuals and the notification process they will follow.

Other considerations

Customers should consider the specific requirements that apply to them, including any industry specific requirements. The relevant privacy and data protection laws and regulations applicable to individual customers will depend on several factors including where a customer conducts business, the industry in which they operate, the type of content they wish to store, where or from whom the content originates, and where the content will be stored. Customers concerned about their privacy regulatory obligations should first ensure they identify and understand the requirements applying to them and seek appropriate advice.