S-DRIVE

CyanGate

S-Drive Security Whitepaper

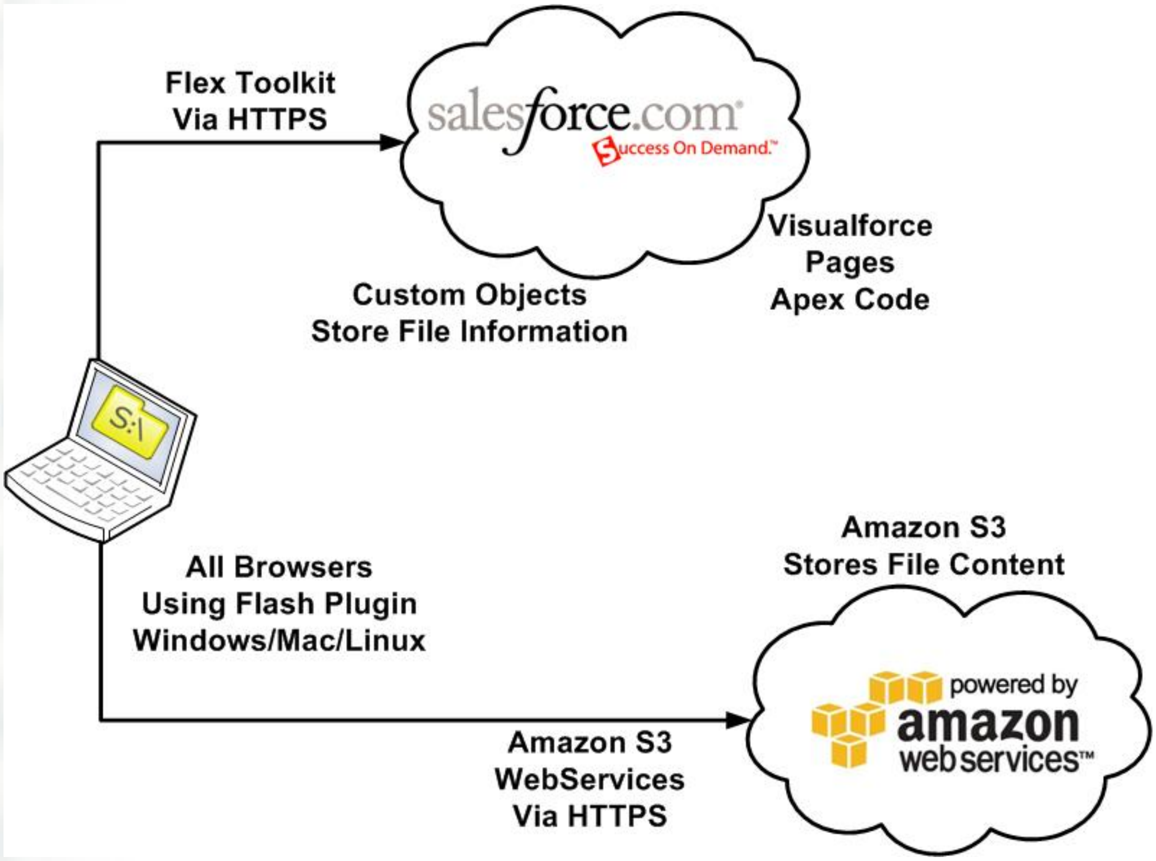
Introduction

S-Drive is a cloud file management solution built on Salesforce.com and Amazon Web Services. S-Drive has been architected with Security and Scalability in mind making it the ideal solution for enterprises and small businesses storing critical business content on the cloud.

S-Drive has been built on Salesforce.com as a managed application and delivered exclusively via the AppExchange marketplace. It is a native AppExchange application meaning that it is built to run in the cloud with multi-tenancy and scalability in mind. S-Drive uses Amazon Simple Storage Service as its file storage platform whereas the Salesforce.com is used as the application platform as well as the file information database. Besides Salesforce.com and Amazon Web Services, S-Drive does not use any other servers or infrastructure that may introduce security vulnerabilities.

Architecture

In order to scale and handle unlimited amount of content, S-Drive has been built on the Salesforce.com platform. The following diagram depicts the architecture of S-Drive storage platform.



The following sections describe the individual components used in the above architecture diagram and explain the security features of each component.

User's Browser

Users interact with S-Drive through their web browser. In order to support user-friendly upload options, S-Drive leverages several options:

- HTML5 upload widget: This widget uses Salesforce.com Ajax calls and Amazon S3 POST API to upload files natively using the latest browser features.

- Adobe Flash plugin: Flash plugin is still kept as an option in case the users face issues due to lack of HTML5 support on their browsers. Flash plugin that is used to upload files directly to Amazon Storage using the Amazon POST API. Also, Flash plugin leverages the Salesforce.com Flex Toolkit to communicate back to Salesforce.com.

- Java Applet: Although Java Applets have been considered insecure due to its access permissions on users' desktops, S-Drive's Java Applet is signed and securely maintained. Java Applet provides a more robust upload feature where multi-threading, checksum verifications and retry mechanisms are supported.

All upload widgets communicate with Salesforce.com as well as Amazon Web Services using secure HTTPS protocol. Any content leaving user's desktop is sent over to its destination using encrypted connection and any content that is downloaded to user's desktop is forced to be transferred using encrypted HTTPS protocol.

Salesforce.com

S-Drive uses Salesforce.com as an application platform. Salesforce.com provides the infrastructure for running S-Drive's business logic and stores the information about the user's files. Since S-Drive has been built on Salesforce.com platform, all user information, authentication and authorization tasks and file level sharing data is handled within Salesforce.com platform. S-Drive uses a combination of Visualforce pages and Apex code (Salesforce.com native programming language) to fulfill user requests.

As of 2014, more than 100,000 businesses with more than 2 million users rely on Salesforce.com with their critical business data. Salesforce.com uses the latest firewall protection, intrusion-detection systems, and TLS (Transport Layer Security) encryption to achieve a secure platform for their customers. Salesforce.com infrastructure has been awarded with certifications such as ISO 27001, the SysTrust audit (the recognized standard for system security), and SysTrust SAS 70 Type II (an attestation for internal corporate controls).

Salesforce.com also provides application level security. Salesforce.com protects customer data by ensuring that only authorized users can access it. Administrators assign data security rules that determine which data users can access. Sharing models define company-wide defaults and data access based on a role hierarchy. All data is encrypted in transfer. All access is governed by strict password security policies. All passwords are stored in MD-5 hash format. Applications are continually monitored for security violation attempts.

Salesforce.com security standards are on par with the best civilian data centers in the world, including the world's most security-conscious financial institutions. Authorized personnel must pass through five levels of biometric scanning to reach the Salesforce.com system cages. All buildings are completely anonymous, with bullet-resistant exterior walls and embassy-grade concrete posts and planters around the perimeter. All exterior entrances feature silent alarm systems that notify law enforcement in the event of suspicion or intrusion. Data is backed up to disk and to tape, with tape providing a second level of physical protection. Neither disks nor tapes ever leave the data center.

Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only http and https traffic on ports 80 and 443, along with ICMP traffic. Switches ensure that the network complies with the RFC 1918 standard, and address translation technologies further enhance network security. IDS sensors protect all network segments. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls points of entry. All networks are certified through third-party vulnerability assessment programs.

Amazon Web Services

S-Drive uses Amazon Web Services to provide storage, billing, Attachment Sync and payment services.

powered by amazon web services™

Amazon Payments Service

S-Drive uses the Amazon Payments service in order to collect S-Drive usage fees from its customers. The payment service provides secure and convenient way for S-Drive customers to automatically pay for the S-Drive usage fees at the end of the month based on the usage statistics gathered by S-Drive throughout the month. Amazon Payments system also provides S-Drive to avoid storing customer financial information such as Credit Card payments. Amazon Payments is Level 1 compliant under the Payment Card Industry (PCI) Data Security Standard (DSS). Use of Amazon Payments provides a piece of mind while providing your Credit Card information and personal information. CyanGate only accesses the unique identifier for the customer’s Amazon Payments account, name and email address and never has access to critical financial data.

Amazon Simple Storage Service (S3)

S-Drive communicates with Amazon Web Services using the REST based APIs. All API calls are executed using HTTPS protocol in order for the data to be encrypted while in transit. In addition all API calls are signed by an HMAC-SHA1 signature with an expiration token.

AWS has in the past successfully completed multiple SAS70 Type II audits, and as of September 30, 2011 publishes a Service Organization Controls 1 (SOC 1) report, published under both the SSAE 16 and the ISAE 3402 professional standards. In addition, AWS has achieved ISO 27001 certification, has been successfully validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS), and has received FISMA-Moderate Authority to Operate.

AWS also provides coverage for U.S. Health Insurance Portability and Accountability Act (HIPAA). AWS enables covered entities and their business associates subject to HIPAA to leverage the secure AWS environment to process, maintain, and store protected health information. Additionally, AWS, as of July 2013, is able to sign business associate agreements (BAA) with such customers.

Amazon has many years of experience in designing, constructing, and operating large-scale data centers. AWS infrastructure is housed in Amazon-controlled data centers throughout the world. Only those within Amazon who have a legitimate business need to have such information know the actual location of these data centers, and the data centers themselves are secured with a variety of physical controls to prevent unauthorized access.

With any shared storage system, the most common security question is whether unauthorized users can access information either intentionally or by mistake. S-Drive uses Amazon's Access Control List to give only Private access to any content uploaded into the S-Drive storage. Private access prevents any unauthorized access to content stored on S-Drive. During access to the content, Amazon authenticates the requests by using the HMAC-SHA1 signature that is supplied by the requestor using the user's private key.

For maximum security, Amazon S3 is accessible via encrypted TLS endpoints from the Internet as well as within the S3 infrastructure. Securing data at rest involves physical security and data encryption. Amazon employs multiple layers of physical security measures to protect customer data at rest. For example, physical access to Amazon datacenters is limited to an audited list of Amazon personnel. Encryption of sensitive data is generally a good security practice; therefore Amazon also provides *server-side encryption at rest* option for each file that is uploaded to S3 using AES256 level encryption. This option is leveraged by S-Drive and allows S-Drive customers to encrypt all of their data while being stored on Amazon storage.

When an object is deleted from Amazon S3, removal of the mapping from the public name to the object starts immediately, and is generally processed across the distributed system within several seconds. Once the mapping is removed, there is no remote access to the deleted object. The underlying storage area is then reclaimed for use by the system.

Amazon S3 is designed to provide 99.999999999% durability and 99.99% availability of objects over a given year. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 Region. To help provide durability, Amazon S3 PUT and COPY operations synchronously store your data across multiple facilities before returning SUCCESS. Once stored, Amazon S3 helps maintain the durability of your objects by quickly detecting and repairing any lost redundancy. Amazon S3 also regularly verifies the integrity of data stored using checksums. If corruption is detected, it is repaired using redundant data. In addition, Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data.

Application Security

Salesforce.com platform provides the application layer for S-Drive. S-Drive is installed as a managed package to customers' organizations and CyanGate maintains the code. S-Drive application code is not visible to end-users and is not exposed by Salesforce.com to the customers. This adds additional security to the application.

S-Drive does not store any customer password in the system. All access to the content is handled by signing requests using an access key and secret key that has been provided by the customers during the installation of the S-Drive AppExchange managed package. These keys are stored in the Salesforce.com protected custom settings and are not accessible by end users. In addition, CyanGate does not access this information or copy this information to any other system. Therefore, at any time, no other organization including CyanGate has access to this critical piece of information. This ensures that only the Customer has access to their data stored in S-Drive.

S-Drive also provides an optional feature called Attachment Sync. This feature allows the standard Salesforce.com attachments to be seamlessly moved to the S-Drive storage. Servers maintained by CyanGate within Amazon’s infrastructure handle this functionality. CyanGate runs security tests against these applications and leverages firewalls provided by Amazon to prevent access to these servers. In addition, customers’ secret keys are never transferred to these servers.

S-Drive’s attachment sync process simply copies files from Salesforce.com to Amazon S3 storage. During this process S-Drive ensures that the files are never written to the file system but instead kept in memory in a transient state. This ensures that customer data is never written to disk.

S-Drive's billing system and registration system is also a portal application that is run on Amazon elastic cloud instances. These systems access customer's Salesforce.com organizations periodically to calculate the storage utilization of S-Drive. During this process, only file sizes are retrieved and stored in S-Drive's database. This information is then used for monthly billing calculations.

S-Drive's billing system requires its customers to provide access to their Salesforce.com organizations. The authentication against the Salesforce.com organization uses oauth authentication scheme and stores the refresh tokens in an encrypted fashion in the database. S-Drive is considered as a connected app with respect to Salesforce.com and the customer, from their Salesforce.com instances, can always terminate access rights for the connected app.

Since S-Drive is sold through the AppExchange marketplace, every year a through source code vulnerability and security audit is executed by Salesforce.com. In addition, an automated code scan (using CheckMarx scanning technology) is executed when a new version of S-Drive is about to be released on the AppExchange and CyanGate is informed on the following security aspects:

- ✓ Cross Site Scripting
- ✓ SOQL Injection
- ✓ SOSL Injection
- ✓ Frame Spoofing
- ✓ Access Control Issues
- ✓ Hardcoded Passwords
- ✓ Open Redirects
- ✓ CRUD/VLS Violations

CyanGate will then address any of these violations and ensure the released code conforms to all of the standard security practices.

In addition to the Application code related security assurances, S-Drive also provides security of content within the organization. This access can be based on two levels of security:

File Level Security

Each file that is stored in S-Drive is represented with a data record in Salesforce.com. Each record is then governed by the sharing rules that are defined in Salesforce.com. S-Drive respects the sharing rules defined on the file record and determines the access rights accordingly. All of the access right information is configurable record by record using the standard Salesforce.com sharing rules.

Profile Level Security

A user profile contains user permissions and access settings that control what users can do within Salesforce.com, the Partner Portal, and the Customer Portal. User Profile determines what level of access is given to a user on any object. The levels include: create, read, edit and delete. Based on the user's profile, S-Drive also determines what access level should be given to a type of file. All profile access permissions are configured through standard Salesforce.com profile administration mechanisms.

Conclusion

S-Drive has been built as a storage platform with the highest level of security and enterprise needs in mind. Although majority of the security provided in S-Drive is provided by Amazon Web Services and Salesforce.com, S-Drive provides a unique architecture in the market to combine these superior platforms and provide a best in class solution.

This paper provides a high level security assessment of S-Drive storage platform. Additional details of security features can be found in references below as well as by contacting S-Drive sales at sdrive@cyangate.com.

References

Amazon Security and Compliance Center

http://aws.amazon.com/security/

Amazon Web Services: Risk and Compliance Whitepaper

https://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf

Amazon Web Services: Overview of Security Processes

http://d36cz9buwru1tt.cloudfront.net/pdf/AWS_Security_Whitepaper.pdf

Salesforce.com Trust Site Security Details

https://trust.salesforce.com/trust/security/

Amazon Simple Storage Service

http://aws.amazon.com/s3/

Salesforce.com Flex Tookit

https://wiki.apexdevnet.com/page/AIR_and_Flex_Toolkit