Neilon Technologies LLP

SECURITY OVERVIEW FOR NEILON TECHNOLOGIES'S PRODUCT S3-LINK

IMPORTANT - READ CAREFULLY: This document is provided for informational purposes only. It represents NEILON’s current security offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of NEILON’s products or services, each of which is provided “as is" without warranty of any kind, whether expressed or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from NEILON, its affiliates, suppliers or licensors. This document is not part of, nor does it modify, any agreement between NEILON and its customers..

S3-Link uses Amazon Web Services (AWS), which delivers a scalable cloud computing platform with high availability and dependability, providing the tools that enable customers to run a wide range of applications. Helping to protect the confidentiality, integrity, and availability of their customers’ systems and data is of the utmost importance to NEILON, as is maintaining customer trust and confidence.

Security in the cloud is slightly different from security in your on premises data centers. When you move computer systems and data to the cloud, security responsibilities become shared between you and your cloud service provider. In this case, AWS is responsible for securing the underlying infrastructure that supports the cloud, and you’re responsible for anything you put on the cloud or connect to the cloud. This shared security responsibility model can reduce your operational burden in many ways, and in some cases may even improve your default security posture without additional action on your part.

AWS Security Responsibilities

Amazon Web Services is responsible for protecting the global infrastructure that runs all of the services offered in the AWS cloud. This infrastructure comprises the hardware, software, networking, and facilities that run AWS services. Protecting this infrastructure is AWS’s number one priority, and while you can’t visit AWS data centers or offices to see this protection firsthand, they provide several reports from third-party auditors who have verified their compliance with a variety of computer security standards and regulations (for more information, visit aws.amazon.com/compliance). Note that in addition to protecting this global infrastructure, AWS is responsible for the security configuration of its 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. For most of these managed services, all you have to do is configure logical access controls for the resources and protect your account credentials.

Customer Security Responsibilities

AWS products that fall into the well-understood category of Infrastructure as a Service (IaaS)—such as Amazon EC2, Amazon VPC, and Amazon S3—are completely under your control and require you to perform all of the necessary security configuration and management tasks. These are basically the same security tasks that you're used to performing no matter where your servers are located. With managed services, you don't have to worry about launching and maintaining instances, patching the guest OS or database, or replicating databases—AWS handles that for you. But as with all services, you should protect your AWS Account credentials and set up individual user accounts with Amazon Identity and Access Management (IAM) so that each of your users has their own credentials and you can implement segregation of duties. AWS also recommends using multi-factor authentication (MFA) with each account, requiring the use of SSL/TLS to communicate with your AWS resources, and setting up API/user activity logging with AWS CloudTrail.

NEILON Security Responsibilities

NEILON's software product S3-Link is built on Force.com platform and uses AWS. Here is the list of items that we consider as our security responsibilities.

1. **AWS IDENTITY & ACCESS MANAGEMENT.** AWS provides a centralized mechanism called AWS Identity and Access Management (IAM) for creating and managing individual users within your AWS Account. A user can be any individual, system, or application that interacts with AWS resources, either programmatically or through the AWS Management Console or AWS Command Line Interface (CLI). Each user has a unique name within the AWS Account, and a unique set of security credentials not shared with other users. AWS IAM eliminates the need to share passwords or keys, and enables you to minimize the use of your AWS Account credentials. With IAM, you define policies that control which AWS services your users can access and what they can do with them. You can grant users only the minimum permissions they need to perform their jobs. NEILON respects all these AWS IAM user and bucket policies. Before using any Amazon user's credentials in Salesforce, customers must implement segregation of duties for that user through Identity and Access Management (IAM).

Customers must configure user and bucket policies to grant/revoke access for different AWS actions and resources.

2. **AWS ACCESS KEYS**. AWS requires that all API requests be signed—that is, they must include a digital signature that AWS can use to verify the identity of the requestor. Digital signature can be calculated using a cryptographic hash function. The input to the hash function in this case includes the text of your request and your secret access key. NEILON uses only one Amazon account credential (AWS Access Keys) to perform all operations in the customer's Salesforce organization. Because access keys can be misused if they fall into the wrong hands, NEILON saves them in protected Salesforce Custom Setting and does not expose them in code or browser. No one (not even NEILON) will have access to these access keys.
3. **DIGITAL SIGNATURE.** Not only does the signing process help protect message integrity by preventing tampering with the request while it is in transit, it also helps protect against potential replay attacks. A request must reach AWS within 15 minutes of the time stamp in the request. Otherwise, AWS denies the request. NEILON uses the most recent version of the digital signature calculation process which is Signature Version 4, which calculates the signature using the HMAC-SHA256 protocol. Version 4 provides an additional measure of protection over previous versions by requiring that you sign the message using a key that is derived from your secret access key rather than using the secret access key itself. In addition, you derive the signing key based on credential scope, which facilitates cryptographic isolation of the signing key.
4. **DATA TRANSMISSION.** NEILON protects data while in-transit (as it travels to and from Amazon S3). NEILON connects to an AWS access point via HTTPS using Secure Sockets Layer (SSL) to protect data in transit. SSL is a cryptographic protocol that is designed to protect against eavesdropping, tampering, and message forgery.
5. **CLIENT SIDE ENCRYPTION.** NEILON also protects data while in-transit. NEILON uses Client-Side Encryption(AES-128 or AES-256) to protect data while in-transit. It encrypts documents in the local machine before upload starts from Salesforce to Amazon S3. So upload requests to Amazon S3 will always contain encrypted documents.
6. **SERVER SIDE ENCRYPTION.** NEILON also protects data at rest (while it is stored on disks in Amazon S3 data centers). NEILON uses Server-Side Encryption(AES-256 or KMS) to protect data at rest. It requests Amazon S3 to encrypt customer data or files before saving it on disks in its data centers and decrypt it when users download those data or files.
7. **CONFIDENTIALITY.** S3-Link is a Salesforce Native App. It is just a connector between the customer's Salesforce environment and their Amazon S3. No customer data or documents will be stored on Neilon system / server or any other third party system / server. It uses a direct connection between the customer's Salesforce environment and it’s Amazon S3 bucket. Documents will be directly stored in the customer's Amazon S3 bucket. NEILON does NOT transmit/process/store any customer data or documents on NEILON

systems/servers or any other third party systems/servers. Documents will be stored only in the customer's Amazon S3 bucket which they will be able to manage by themselves. And data(metadata of Amazon S3 documents) will be stored only in the customer's Salesforce environment. So no data will go outside of their Salesforce environment.

AWS Compliance Program

Amazon Web Services Compliance enables customers to understand the robust controls in place at AWS to maintain security and data protection in the cloud. As systems are built on top of AWS cloud infrastructure, compliance responsibilities will be shared. By tying together governance-focused, audit friendly service features with applicable compliance or audit standards, AWS Compliance enablers build on traditional programs, helping customers to establish and operate in an AWS security control environment. The IT infrastructure that AWS provides to its customers is designed and managed in alignment with security best practices and a variety of IT security standards, including:

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Level 3

In addition, the flexibility and control that the AWS platform provides allows customers to deploy solutions that meet several industry-specific standards, including:

- Criminal Justice Information Services (CJIS)
- Cloud Security Alliance (CSA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Motion Picture Association of America (MPAA)