SysAid

SYSAID CLOUD SECURITY AND COMPLIANCE STANDARDS

Security is built in throughout SysAid Cloud – in capabilities such as: dealing with failed logins, encrypted password protection, access control rules, and audit logs.

In terms of environment security, SysAid Cloud is hosted in third-party state-of-the-art data centers across four different regions:

USA

US-AWS is hosted on three availability zones in Virginia with Amazon Web Services.

EUROPE

EU-AWS is hosted on three availability zones in Ireland with Amazon Web Services.

ASIA PACIFIC

AU-AWS is hosted on two availability zones in Sydney with Amazon Web Services.

MIDDLE EAST

IL-TC is hosted in Petah-Tikva, Israel with Triple-C.

This security and compliance document relates to SysAid Cloud hosted in AWS environments.

AWS AND SYSAID'S SHARED COMPLIANCE RESPONSIBILITY

AWS Compliance provides assurance related to the underlying cloud infrastructure and SysAid for the SysAid Cloud solution.
So AWS operates, manages, and controls the components from the host operating system and virtualization layer, down to the physical security of the facilities in which the service operates.

SysAid, like any other AWS customer, has responsibility for, and manages: the guest operating system (including updates and security patches), the SysAid Cloud application, and the configuration of the AWS-provided security group firewall.

Furthermore, AWS offers shared responsibility models for each of the different types of services that it offers:

- Infrastructure services
- Container services
- Abstracted services

In the shared responsibility model for infrastructure services, for example, AWS manages the security of the following assets:

- Facilities
- Physical security of hardware
- Network infrastructure
- Virtualization infrastructure

SysAid is responsible for the security of the following assets:

- Amazon Machine Images (AMIs)
- Operating systems
- Applications
- Data in transit
- Data at rest
- Data stores
- Credentials
- Policies and configuration

The following diagram depicts the building blocks for the shared responsibility model for infrastructure services.

More information, including the shared responsibility models for container and abstracted services, can be found in the AWS Security Best Practices document.

SECURITY AND COMPLIANCE STANDARDS

From an AWS hosting perspective, the key certifications include:

SOC 1/SSAE 16/ISAE 3402 (formerly SAS70)

AWS publishes a Service Organization Controls 1 (SOC 1), Type II report. The audit for this report is conducted in accordance with the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) and the International Standards for Assurance Engagements No. 3402 (ISAE 3402).
This replaces the Statement on Auditing Standards No. 70 (SAS 70) Type II report. The SOC 1 report audit attests that the AWS control objectives are appropriately designed and that the controls safeguarding customer data are operating effectively. It includes the three AWS data centers used by SysAid in US East (Northern Virginia), EU (Ireland), and Asia Pacific (Sydney).
Ernst & Young LLP performs the AWS SOC 1, SOC 2, and SOC 3 audits.
Please see Appendix 1 for the AWS SOC 1 control objectives.

SOC 2

Similar to SOC 1 in the evaluation of controls, the SOC 2 report is an attestation report that expands the evaluation of controls to the criteria set forth by the American Institute of Certified Public Accountants (AICPA) Trust Services Principles. These principles define leading practice controls relevant to security, availability, processing integrity, confidentiality, and privacy applicable to service organizations. This report provides additional transparency into AWS security based on a defined industry standard and further demonstrates AWS's commitment to protecting customer data.
The AWS SOC 2 report again includes AWS data centers in US East (Northern Virginia), EU (Ireland), and Asia Pacific (Sydney).

SOC 3

The SOC 3 report is a publicly available summary of the AWS SOC 2 report and provides the AICPA SysTrust Security Seal. The report includes: the external auditor's opinion of the operation of controls (based on the AICPA's Security Trust Principles included in the SOC 2 report); the assertion from AWS management regarding the effectiveness of controls; and an overview of AWS Infrastructure and Services.
The AWS SOC 3 report again includes AWS data centers in US East (Northern Virginia), EU (Ireland), Asia Pacific (Sydney), and South America (Sao Paulo). The AWS SOC 3 is publicly available and can be found here.

ISO 27001

AWS is ISO 27001 certified under the International Organization for Standardization (ISO) 27001 standard. This is a widely-adopted global security standard that outlines the requirements for information security management systems and, in order to achieve the certification, a company must show it has a systematic and ongoing approach to managing information security risks that affect the confidentiality, integrity, and availability of company and customer information. AWS has established a formal program to maintain the certification across the AWS data centers in US East (Northern Virginia), EU (Ireland), and Asia Pacific (Sydney). The certifying agent is EY CertifyPoint, an ISO certifying agent accredited by the Dutch Accreditation Council and a member of the International Accreditation Forum (IAF).

FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP is mandatory for Federal Agency cloud deployments and service models at the low and moderate risk impact levels. AWS is a FedRAMP Compliant Cloud Service Provider (CSP),has completed the testing performed by a FedRAMP-accredited Third Party Assessment Organization (3PAO), and has been granted two Agency Authority to Operate (ATOs) by the US Department of Health and Human Services (HHS) after demonstrating compliance with FedRAMP requirements. Two separate FedRAMP Agency ATOs have been issued; one encompassing the AWS GovCloud (US) Region,and the other covering the AWS US East/West regions.

CSA

In 2011, the Cloud Security Alliance (CSA) launched STAR, an initiative to encourage transparency of security practices within cloud providers. The CSA Security, Trust & Assurance Registry (STAR) is a free, publicly accessible registry that documents the security controls provided by various cloud computing offerings, thereby helping users assess the security of cloud providers they currently use or are considering contracting with. AWS is a CSA STAR registrant and has completed the Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ). The AWS responses to the CSA Consensus Assessments Initiative uestionnaire v1.1 can be found in Appendix A of the AWS Risk and Compliance Whitepaper.

PCI DSS Level 1

AWS is Level 1 compliant under the Payment Card Industry (PCI) Data Security Standard (DSS) such that customers can run applications for storing, processing, and transmitting credit card information in the cloud.

HIPAA

AWS allows organizations subject to the U.S. Health Insurance Portability and Accountability Act (HIPAA) to process, maintain,and store protected health information.

SysAid is happy to provide security and compliance reports and certifications produced by third-party auditors, which attest to the design and operating effectiveness of the AWS environment.

THE AWS CONTROL ENVIRONMENT

AWS manages a comprehensive control environment that includes policies, processes, and control activities for the secure delivery of AWS's service offerings. AWS has integrated applicable cloud-specific controls identified by leading cloud computing industry bodies into the AWS control framework. AWS continues to monitor these industry groups for ideas on which leading practices can be implemented to better assist customers with managing their control environment.

The control environment at Amazon begins at the highest level of the Company. Executive and senior leadership play important roles in establishing the Company's tone and core values. Every employee is provided with the Company's Code of Business Conduct and Ethics and completes periodic training. Compliance audits are performed so that employees understand and follow the established policies.

The AWS organizational structure provides a framework for planning, executing, and controlling business operations. It assigns roles and responsibilities to provide for adequate staffing, efficiency of operations, and the segregation of duties. Management has also established authority and appropriate lines of reporting for key personnel. Included as part of the Company's hiring verification processes are education, previous employment, and background checks as permitted by law and regulation for employees commensurate with the employee's position and level of access to AWS facilities.

The AWS document Security at Scale: Governance in AWS provides additional information, with Amazon stating that AWS offers better security than many on-premise environments through its robust governance framework.

Network Security

Secure Network Architecture

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.

Secure Access Points

AWS has 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). In addition, AWS has implemented network devices that are dedicated to managing interfacing communications with internet service providers (ISPs).

Transmission Protection

You can connect to an AWS access point via HTTP or HTTPS using Secure Sockets Layer (SSL), a cryptographic protocol that is designed to protect against eavesdropping, tampering, and message forgery.

Amazon Corporate Segregation

The AWS production network is segregated from the Amazon corporate network by means of a complex set of network security/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.

Network Monitoring and Protection

AWS utilizes a wide variety of automated monitoring systems to provide a high level of service performance and availability. AWS monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts.

The AWS network provides significant protection against traditional network security issues such as:

- **Distributed Denial Of Service (DDoS) Attacks**
  AWS API endpoints are hosted on large, Internet-scale, world-class infrastructure that benefits from the same engineering expertise that has built Amazon into the world's largest online retailer. Proprietary DDoS mitigation techniques are used. Additionally, AWS's networks are multi-homed across a number of providers to achieve Internet access diversity.

- **Man in the Middle (MITM) Attacks**
  All of the AWS APIs are available via SSL-protected endpoints, which provide server authentication.

- **IP Spoofing**
  The AWS-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.

- **Port Scanning**
  When unauthorized port scanning is detected by AWS, it is stopped and blocked. Port scans of Amazon EC2 instances are generally ineffective because, by default, all inbound ports on Amazon EC2 instances are closed and are only opened by customers.

Information Security

AWS has a formal information security program designed to protect the confidentiality, integrity, and availability of SysAid customers' systems and data. A security whitepaper, available on the Amazon website, details how data is secured.

SysAid Cloud Level Security

Firewalls

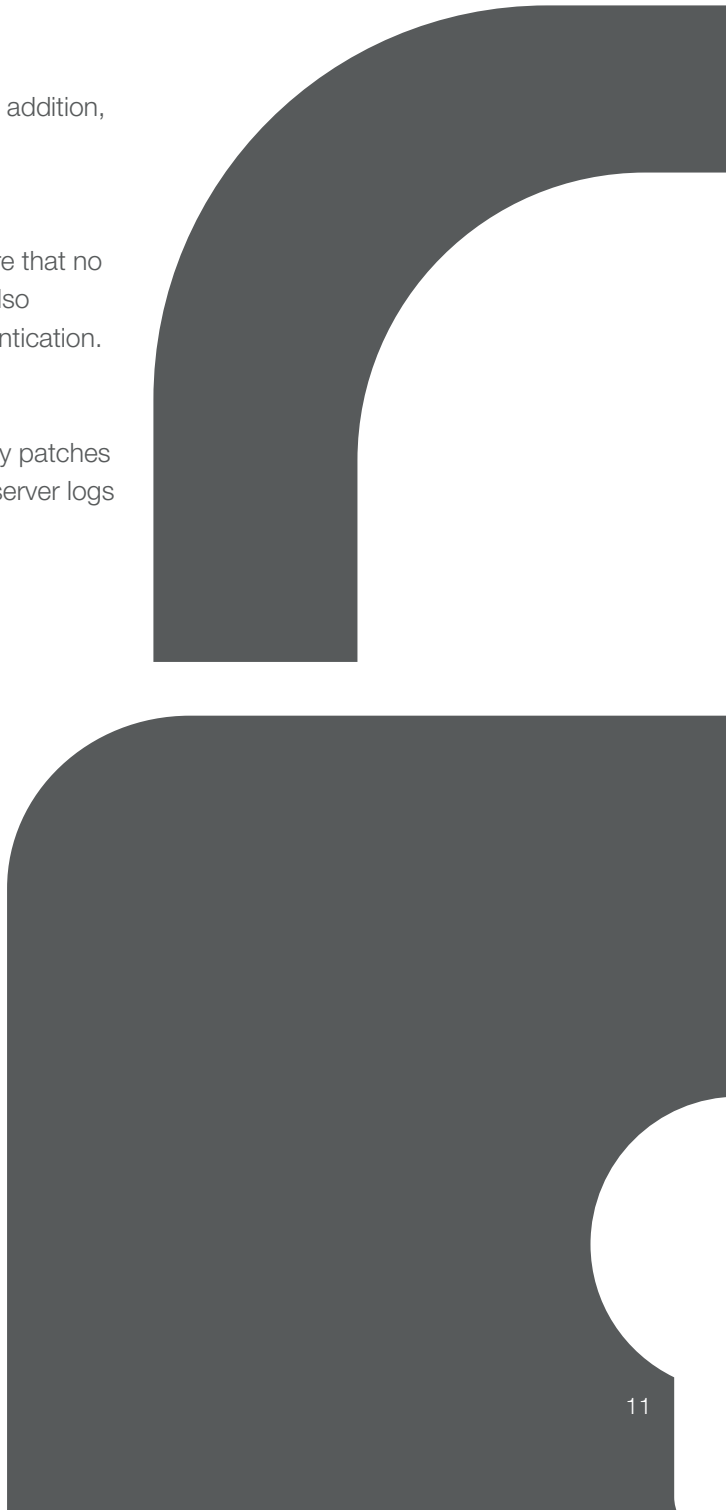
All servers are protected by strict security policies defined in AWS. In addition, each server is also protected with another layer of software firewall.

Network Security

Database and application servers are protected by a firewall to ensure that no unauthorized traffic can reach the servers. Access to the servers is also restricted to approved IP addresses and requires a private key authentication.

Server OS Security

All OS or other back-end patches are applied immediately for security patches and in 1–5 days for non-security patches. Full security audits of the server logs are performed on a periodic basis.



Application Security

- SysAid is (optionally or forcibly) accessible via HTTPS using SSL High-Grade Encryption to ensure that data in-transit is secure.
- Regular and thorough application security testing is performed at all stages of development to ensure that the application interface can't be exploited.
- A complete vulnerability assessment (including penetration testing) on the live environment is periodically performed by external security experts, whose recommendations are constantly implemented within the product and the environment.
- Data for each customer is stored in its own database, ensuring that there is no data leakage.

Human Factor Security

- Access to the servers is restricted to the server administrators, an approved representative of the supportteam, and an approved representative of the development team (access is revoked if no longer necessary).
- In no cases do any of these administrators look at actual customer-entered data without the express written consent of the customer.
- Server logins are reviewed daily.
- Any changes made to the cloud environment follow a predefined change process, including approvals, as specified by ITIL best practices.

APPENDIX 1: AWS SOC 1 CONTROL OBJECTIVES

OBJECTIVE AREA	OBJECTIVE DESCRIPTION
Security Organization	Controls provide reasonable assurance that information security policies have been implemented and communicated throughout the organization.
Amazon User Access	Controls provide reasonable assurance that procedures have been established so that Amazon user accounts are added, modified, and deleted in a timely manner and are reviewed on a periodic basis.
Logical Security	Controls provide reasonable assurance that unauthorized internal and external access to data is appropriately restricted, and access to customer data is appropriately segregated from other customers.
Secure Data Handling	Controls provide reasonable assurance that data handling between the customer's point of initiation to an AWS storage location is secured and mapped accurately.
Physical Security and Environmental Safeguards	Controls provide reasonable assurance that physical access to Amazon's operations building and the data centers is restricted to authorized personnel and that procedures exist to minimize the effect of a malfunction or physical disaster to the computer and data center facilities.
Change Management	Controls provide reasonable assurance that changes (including emergency/non-routine and configuration) to existing IT resources are logged, authorized, tested, approved, and documented.
Data Integrity, Availability, and Redundancy	Controls provide reasonable assurance that data integrity is maintained through all phases including transmission, storage, and processing.
Incident Handling	Controls provide reasonable assurance that system incidents are recorded, analyzed, and resolved.

Source: AWS Risk and Compliance Whitepaper