Hosted Managed Services for SAS® Technology
Contents

Performance ......................................................................................................................... 1
  Optimal storage and sizing ......................................................................................... 1
  Secure, no-hassle access .......................................................................................... 2
  Dedicated computing infrastructure ....................................................................... 2
  Early and pre-emptive detection of incidents ...................................................... 2

Security ................................................................................................................................. 2
  Data protection warranties (with approved liability levels) for personally identifiable information .......................................................... 3
  Documented data classification and handling policy ............................................. 3
  Continuous improvement efforts ............................................................................ 3
  SOC 2/SOC 3 Type II processes and controls ...................................................... 4
  Site-to-site VPN/IP whitelisting ............................................................................. 4
  Secure FTP with automated data ingestion processes ........................................ 4
  Patching of SAS® solutions where required for security ..................................... 4
  Access control and account management ............................................................. 5
  Robust sub-contractor qualification and management .......................................... 5

Service Operation Management ....................................................................................... 5
  Event management ...................................................................................................... 5
  Incident management ................................................................................................ 5
  Problem management ............................................................................................... 5

Stability ................................................................................................................................. 6
  Best-practice installation of SAS® software .......................................................... 6
  Incident response targets ........................................................................................ 6
  Data centers: Tier 2 or higher .................................................................................... 7
  Defined standards and documentation for SAS® installations .......................... 7
  Monitoring and alerting of storage capacity configured to SAS® ...................... 7
  Backup of all key data ............................................................................................... 7
  SAS Continuity of Business Program ................................................................... 8

Conclusion ......................................................................................................................... 8
Hosted managed services is an excellent option for organizations looking for a comprehensive analytics solutions based on SAS® industry-leading products – and delivered by the insiders who know these tools best. Hosted managed services give you the option to deploy the technology on an infrastructure that has been tuned specifically for the solution.

Hosted SAS solutions are housed in any of SAS hosting centers or selected cloud providers across the globe. Due to the combination of cutting-edge technology and dedicated service and support, SAS hosted managed services have helped customers:

- **Reduce capital costs.** Organizations can save money by skipping large, upfront hardware purchases – and enjoy more predictable costs over time. Therefore, you get superior analytics and business intelligence solutions that drive bottom-line results.

- **Increase staffing savings.** With a SAS hosted solution, you can reduce your reliance on already overtaxed internal staffing resources. Rely on SAS to provide expert capacity planning and support – and let your staff focus on proactive business improvement.

- **Reduced operational costs.** With no installation of software or hardware at the customer site, you can see energy savings as well as improved performance.

This paper highlights the primary advantages of choosing SAS as your hosted managed services provider. The paper concentrates on four main areas where your organization benefits from SAS hosted managed services: performance, security, service operation management and stability.

### Performance

Performance is one of the main reasons customers rely on SAS for hosted managed services. With this deployment method, you get dedicated infrastructure, optimal hardware sizing and tailored alerting. Here’s how SAS delivers exceptional performance through its hosted managed services:

**Optimal storage and sizing**

Choosing a hosted managed services solution means you receive the benefit of SAS’ experience to configure the optimal hardware for your SAS hosted applications and solutions. This is critical for industries or use cases that involve large volumes of data. Big data deployments are notoriously difficult to maintain from an infrastructure perspective.

SAS has experts that can determine what infrastructure each solution needs to perform effectively and efficiently. By selecting SAS hosted managed services, you can use that experience from the SAS team to specify the right hardware and associated disk space that will achieve the ideal performance for your hosted solution.
Secure, no-hassle access

With SAS hosted managed services, the customer just provides a web browser or a remote desktop connection client – SAS takes care of everything else. This gives you a “right-sized” terminal server and installation of SAS client software – including all prerequisite third-party software. Customers rely on SAS expertise to handle:

- All prerequisites.
- The installation of all required client and server software.
- The setup of all third-party software applications necessary to operate with the SAS solution.

Dedicated computing infrastructure

By working with SAS, be confident you have dedicated infrastructure to support the hosted managed services solution – with no “over-provisioning” of virtual machines. The hardware capacity purchased to run your SAS solution is not shared with any other organization.

At the core of all SAS solutions is the ability to handle large data volumes. SAS understands that these solutions require more power and infrastructure to support them. SAS hosted managed services harness the power you need to run your analytic solutions at the highest levels of efficiency.

Early and pre-emptive detection of incidents

SAS understands how to monitor SAS solutions to achieve the thresholds required for optimal performance. For your hosted managed service, SAS can then apply that expert knowledge to set up the most effective monitoring and alerting framework for your solution. As your solution grows and changes over time, SAS adjusts these monitors and alerts, when necessary, to ensure the solution retains optimal performance.

Hosted managed services customers benefit from the best SAS solution working in tandem with the most optimally performing infrastructure. SAS understands how to set up its customers’ solutions in the beginning and maintain the infrastructure at the peak level of performance throughout the life cycle.

Security

SAS has experience with hosting sensitive data for organizations around the world. SAS provides hosted managed services for customers in many sectors, including government, financial services, pharmaceuticals and health care.

For all hosted managed services, SAS offers security across major areas:

- Physical – video surveillance, barriers to entry, and card access.
- Logical – network, database, operating system and application.
- Personnel access – Use of user ID and password as well as training.
Data protection warranties (with approved liability levels) for personally identifiable information

SAS understands the importance of data protection, especially in the world of hosted services. Data protection is a significant step in an organization’s due diligence process when selecting a company to host its solution. SAS takes every precaution to protect its customers.

SAS provides contractual guarantees to its customers for all non-public data collected and maintained in any of its data centers. SAS maintains robust and fit-for-purpose technical and organizational approaches to security for its hosted managed services solutions. Liability levels are agreed upon according to each customer’s requirements.

Documented data classification and handling policy

When implementing hosted managed services, SAS works with customers to determine the most appropriate data classification level for information hosted in each solution. Customers classify their data in SAS custody, or under its control into one of four levels: public, internal use only, confidential and restricted. SAS has standardized procedures for handling customer data at each level of classification. All staff receives training on data classification and handling policies before working on hosting managed services solutions.

Continuous improvement efforts

SAS hosts solutions for privacy-conscious industries. As a result, SAS’ security policies and controls are regularly audited by third parties, including customers and SAS’ own auditors. This allows SAS to maintain its certifications (Service Organization Controls, like SOC 2 and SOC 3). By committing to regular audits, any potential improvements to SAS security process may be highlighted and fed into continuous service improvement projects.

SAS Solutions OnDemand additionally regularly engages third-party consultants to assess its methodologies, with the goal of aligning to best practices and standards, as well as optimizing service delivery and providing continual improvement.

SAS also monitors external standards, best practices and industry and regulatory requirements that may be applicable to its customers and may benchmark its policies and standards against relevant third-party or government frameworks. Third-party and regulatory frameworks and standards that SAS may consider for a given customer implementation include the following:

- National Institute of Standards and Technology (NIST: SP 800-53 Rev. 4; NIST SP 800-171).

- International Organization of Standardization (ISO: 27001 ISO 20000).

- Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act.

- Information Technology Infrastructure Library (ITIL).

SAS has experience hosting sensitive data for organizations across a wide variety of sectors globally, including government, banking/financial services, pharmaceuticals and health care.
SOC 2/SOC 3 Type II processes and controls

SOC reports are designed to help service organizations operate information systems and provide information system services to other entities. They also help build trust and confidence in their service delivery processes and controls through a report by an independent, certified public accountant.

SAS performs an annual SOC 2 Type 2 and SOC 3 audit engagement, using independent service auditors in accordance with AT section 101, Attest Engagements, under the guidance provided in Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy. The audit reports demonstrate that SAS controls satisfy the trust services criteria of security and availability with respect to customer data that is stored and processed using SAS Solutions OnDemand hosted solutions.

There are two types of SOC 2 reports. SAS delivers a Type 2 report, which offers a description of SAS’ hosting system and the suitability of the design and operating effectiveness of controls. SAS also offers a SOC 3 report, which provide only the auditor’s summary on whether the system achieved the trust services criteria, which include security, availability, processing integrity, confidentiality and privacy.

These reports, which can be provided to customers subject to the execution of an appropriate nondisclosure agreement, confirm that SAS Solutions OnDemand has effective procedures and controls in place to deliver reliable, safe and secure services. Global SAS data centers may have other certifications where applicable and appropriate.

Site-to-site VPN/IP whitelisting

SAS requires site-to-site or whitelisted IPs when providing customers with access to their hosted managed services solutions in accordance with contract language. This approach prevents the visibility of SAS’ presence online, reducing the opportunity for hacking attacks. If the SAS solution does not recognize the IP of the individual attempting to access the solution, it denies the individual access.

Secure FTP with automated data ingestion processes

Because data sits at the heart of analytics, it is crucial for SAS to provide a secure method for receiving data into the system. SAS offers multiple methods for reliable, secure electronic file transfer, including FTP over SSL (FTP/S), secure file transfer protocol (SFTP) and hypertext transfer protocol secure (HTTPS). These methods ensure that files are encrypted in transit as they move from the customer to SAS over unsecured networks, and they have the benefit of simple auditability. SAS provides tools and best practices to enable its customers to use these file transfer methods quickly and easily.

Patching of SAS® solutions where required for security

SAS tests its software and customers’ hosting infrastructure for security vulnerabilities. In addition, SAS subscribes to daily threat notices from external sources to keep up to date on security threats in the industry. If any vulnerabilities are identified, SAS implements patches to address these vulnerabilities and reduce the risk of security incidents.
Access control and account management

SAS controls the authorization for access, disclosure, duplication, modification, diversion, destruction, loss, misuse or theft of information stored in the hosted environment. Access and authorization is based on the security principles of least privilege and the need to know. SAS maintains a secure environment through access control and account management policies and processes.

The SAS hosted managed services environment requires user authentication and authorization. SAS or customer-delegated administrators (as applicable to the hosted application or applications) manage accounts, passwords and permissions to ensure that all users are properly identified and authenticated when accessing the SAS hosted managed services environment. The combination of a unique user ID and a valid password is the minimum requirement for granting access to an information system.

Robust subcontractor qualification and management

Whenever SAS subcontracts any services to a partner, SAS follows its Supplier Qualification and Management Program, including initial evaluation, approval, disapproval and continuous improvement and management of its supplier base. While this program applies to onboarding new subcontractors, SAS also conducts regular risk assessments to ensure partners continue to meet SAS’ required service and security levels. It is SAS policy that customer material be encrypted while in transit and at rest, whenever possible.

Service Operation Management

Service operation management coordinates and executes the required activities and processes to ensure that SAS solutions are available and performing 24/7. Service operation includes event management, incident management and problem management.

Event management

An event may indicate something is not functioning correctly, leading to the logging of an incident. Events may also indicate normal activity or a need for routine intervention. Event management depends on monitoring, but it goes beyond that. Event management generates and detects notifications, while monitoring checks the status of components even when no events are occurring. After an event is detected, it may lead to incident management, problem management or change management. Alternatively, it may simply be logged in case the information is needed. Response to an event can be automated or can require manual intervention.

Incident management

The objective of incident management is to restore normal service operation as quickly as possible and minimize the adverse effect on business operations. This keeps things running at the best possible levels of service quality, helping to keep availability levels high.

Problem management

Problem management helps to identify the cause of an error in the SAS software and infrastructure that is usually reported as occurrences of related incidents. Resolving a problem leads to addressing the error that prohibits related incidents from occurring in the future.
Stability

Customers choose hosted managed services to guarantee solution availability at all times. SAS offers various levels of stability - ranging from 99 percent warranty, best-practice installation, provisioning of all third-party software and incident response times.

SAS guarantees 99 percent uptime on all SAS software for hosted managed services. SAS views the uptime of its software as part of the overall IT ecosystem. As shown in Figure 1, the SAS software availability relies on uptime of all hosted managed services areas, including database management services, IT services, operating systems, infrastructure, data centers and more.

Best-practice installation of SAS® software

To optimize performance, stability and security, SAS uses its own expertise and best practices to install the SAS solution. All SAS software is installed according to a set of common standards. This means any technical support staff member can answer customer questions and resolve issues quickly.

Incident response targets

For any incident affecting software availability, SAS alerts its hosted managed services customers based on agreed-upon capacity thresholds. This ensures customers receive timely communications. As a result, customers have confidence that SAS can appropriately manage any type of incident level.
The priority of an incident is based on impact (does it affect the entire environment, part of the environment or one or more users) and urgency (how long the incident has a significant impact on the customer’s environment). The priority determines response and recovery planning. SAS maintains regular customer communications while resolving the incident.

For more major incidents that indicate the possibility of an underlying problem, SAS performs a root cause analysis with the objective of preventing a recurrence of the incident.

Data centers: Tier 2 or higher

The Uptime Institute is a two-decade-old advisory organization focused on improving the performance, efficiency and reliability of business-critical infrastructure through innovation, collaboration and independent certifications.

The Uptime Institute created the standard Tier Classification System to effectively evaluate data center infrastructure in terms of a business’ requirements for system availability. The Tier Classification System provides the data center industry with a consistent method to compare typically unique, customized facilities based on expected site infrastructure performance or uptime. Furthermore, tiers enable companies to align their data center infrastructure investment with business goals specific to growth and technology strategies. All SAS data centers are Tier 2 or higher.

The Uptime Institute reviews and approves Facilities, Operations, Efficient IT and FORCSS (Financial, Opportunity, Risk, Compliance, Sustainability and Service Quality).

Defined standards and documentation for SAS® installations

All implementations, batch jobs and ETL jobs are handled following the same standards and documented following the same process, providing standardization and common sharing of information across the team. This means that any of the support staff can manage any issues and respond efficiently and effectively.

SAS uses a common documentation system to manage all hosted managed services solutions. This installation and configuration documentation serves as a tool for rapid issue diagnosis and resolution.

Monitoring and alerting of storage capacity configured to SAS®

SAS uses systems to monitor its customer’s storage capacity. The monitoring systems SAS uses include advanced warning flags to ensure stability to prevent its customers from experiencing any system degradation.

Backup of all key data

SAS backup data is moved off-site to provide a fallback for resilience purposes. If a major incident occurs, as a last resort SAS may have to restore the solution from its latest backup.
SAS Continuity of Business Program

SAS maintains a Continuity of Business (COB) Program aimed at protecting its key assets and continuing its critical business functions upon the occurrence of a disruptive incident. The SAS COB Policy provides a layer of program governance, formalizing roles and responsibilities and standardizing specific activities including annual plan maintenance and testing, staff training and management program review. For additional information regarding SAS’ COB Program, refer to the Continuity of Business white paper.

Conclusion

SAS offers its core capabilities within its hosted managed services offering. Performance, security, operation management and stability are the core deliverables SAS customers have come to rely upon the SAS team to deliver with any hosted managed service deployment.

If you would like more information on anything contained within this paper, please contact your local SAS Solutions OnDemand representative.