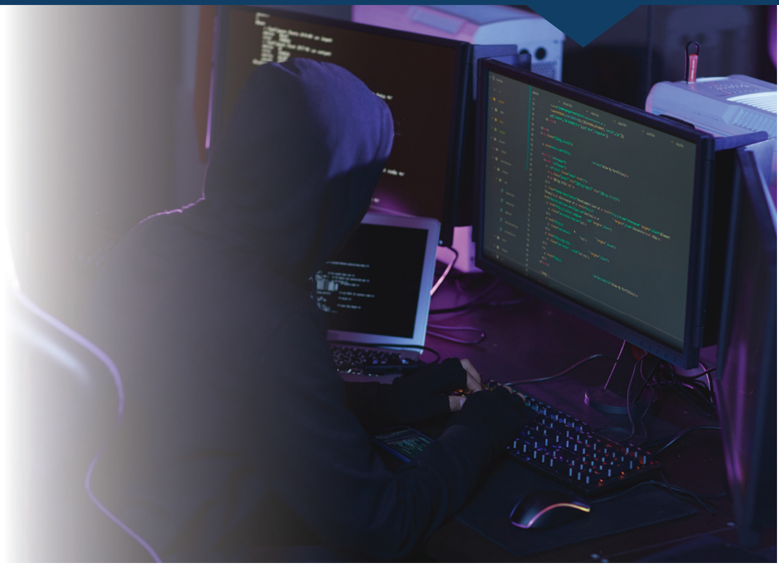
SAP NS2 Secure Cloud

Ensuring you have the relevant security controls to fulfill the security regulations that are required of your organization

In today's ever-changing cyber landscape, threats are constantly evolving and growing. Nation-states and hackers all over the world are targeting organizations every moment.

Organizations need assistance with the different regulations they need to comply with in order protect their critical networks. There are multiple regulations and frameworks (i.e., FedRAMP, NIST, ITAR, HIPAA, GDPR and SOX) that may be required, often with overlapping requirements.



> **Effective cloud security needs to incorporate a multitude of procedures and strategies in order to rise above the dangers in the digital landscape.**

Why SAP NS2?

SAP NS2's Secure Cloud provides a solution for customers to run their mission critical systems. We leverage our unique position, as both a large US defense contractor and a commercial cloud provider, to bring a level of security to our commercial customers and US Five Eyes partners.

SAP NS2 has invested heavily in technology, resources and inspections to safeguard your digital assets in our cloud solutions. Partnering with SAP NS2 will ensure that you have the relevant security controls to fulfill the security regulations that are required of your organization. SAP NS2's enterprise security strategy provides constant safeguards that directly benefit our customers and provide integrated layers of protection to detect and resolve any threats impacting your organization. Our success is propelled by the need to innovate faster than external threats while enabling our teams that are driven to defend.

SAP NS2 Secure Cloud Discrete Discriminators

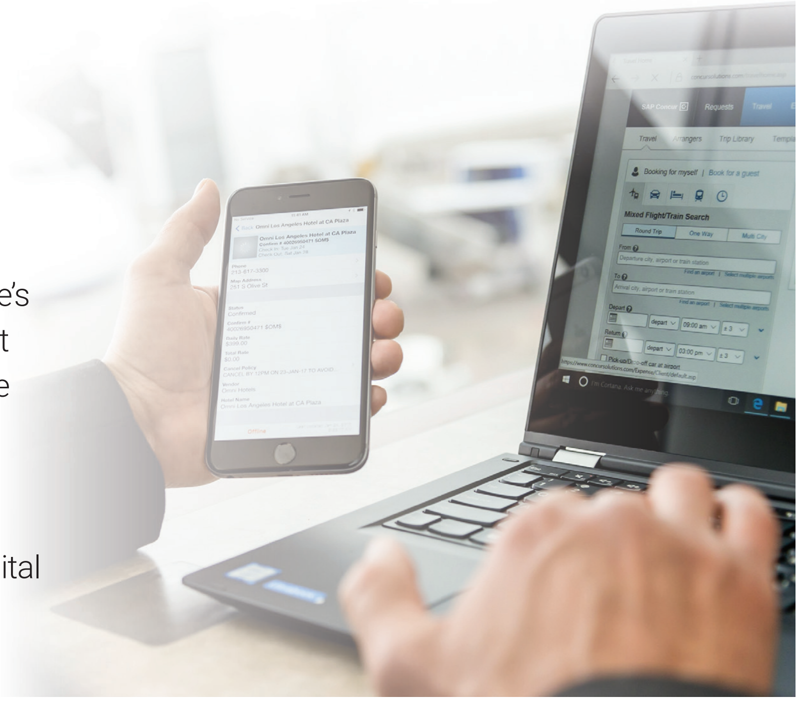
- Operate cloud services and support from secure DoD compliant facilities
- Applications on the most secure infrastructure that the various hyperscalers have to offer
- Security monitoring and patching across the cloud environments
- 100% U.S. persons hired with background checks
- Common security controls applied across all cloud environments — government and commercial
- Continuous monitoring, detection and remediation

A security strategy needs to leverage innovation and resources for absolute protection. From an innovation standpoint, it is about detection and prevention. Identifying threats and bad actors require solution level detection across the entire stack of capabilities. Threats can hide in the network, operating system, data and the application. A monitoring strategy needs to have an automated way to detect these threats while also examining the performance of these solutions to meet the needs of your stakeholders. Our **Security Information and Event Management (SIEM)** systems alert, monitor, analyze and verify potential security attacks on and technical disruptions of SAP NS2's Cloud environments and we log the necessary information to protect all critical systems and infrastructure components. In order to enable these types of protections, the cloud solution needs to incorporate these mechanisms in every facet of the solution creation. This is not a capability that a customer "turns on." This protection is built into the fabric of every layer of the SAP NS2 Cloud solutions. These are fundamental components to protect and support our customers while remaining relentless in our pursuit to defend.

At SAP NS2, our cloud solutions are designed to provide physical and logical separation of your data and digital assets. Protection and exposure for our customers is a fundamental component of our security landscape and administrative networks are completely separated from customer networks. SAP NS2 has established security measures to ensure that our customers cannot access cloud services from other parties. Our solutions meet and exceed enterprise grade cloud capabilities, providing protection from incoming cyber intrusion attempts.

Enterprise Grade Endpoint Security

Endpoint security is another fundamental component of our enterprise security strategy. It provides an additional layer of protection for each user by minimizing the overall security vulnerabilities of the enterprise. Each endpoint represents a connected device (i.e. desktop, laptop, server, mobile device) within an enterprise's network. These endpoints are a significant target for external threats for any enterprise and require specialized levels of fortification to defend your organization. Our SAP NS2 Cloud solutions can provide enterprise grade endpoint security and protection to immediately detect and resolve digital threats and potential weaknesses.



Independent Security Controls

One of the most important components of a cloud security strategy is assurances from auditors and 3rd parties that our protection mechanisms are effective. Federal and Department of Defense customers need to adhere to the necessary security controls set forth by the government to preserve their digital assets.

> **A number of our SAP NS2 Cloud solutions adhere to FedRAMP Moderate controls in order to help ensure that the necessary federal protections are in place to protect and process US Government data.**

The security controls are based upon the National Institute of Standards and Technology (NIST) SP 800-53. These security controls are reviewed and audited by a 3rd Party Audit Organization (3PAO) in order to independently assess that the necessary precautions are implemented correctly.

In addition, our SAP NS2 Cloud solutions adhere to the strict guidelines set forth to protect International Traffic in Arms Regulations (ITAR) related data. ITAR requires that this information not be inadvertently released or distributed to foreign persons or destinations outside the United States. This is critical information that needs to be preserved, protected and geographically isolated to safeguard the essential investments of our customers. Our cloud solutions are independently reviewed by our SAP NS2 Chief Information Security Officer (CISO) in order to self-attest that the appropriate NIST SP 800-53 security controls were implemented correctly.

Staffed with 100% U.S. Persons on U.S. Soil

The most important component of an enterprise grade cloud solution is the resources that support the applications. Cloud applications include business capabilities and support for each customer. At SAP NS2, we make sure that our resources can pass background checks and hold clearances when applicable. We require US persons on US soil to perform the work in the cloud. One of the greatest threats impacting the cloud landscape is that the people managing the systems are unidentifiable to a customer. Our question to you is don't you want to know who is working in your cloud? At SAP NS2, we provide absolute transparency on the resources safeguarding your cloud solutions and they can adhere to your resource guidelines in order to successfully protect your enterprise.

SAP NS2 Commitment to Security

SAP NS2 is a winner of the 2019 Defense Security Service James S. Cogswell Outstanding Industrial Security Achievement Award. The Cogswell award is the most prestigious honor the Defense Security Service may bestow to cleared industry. Of the more than 13,000 cleared contractors, less than one percent are annually selected to receive this award.

JAMES S. COGSWELL AWARD
DEFENSE SECURITY SERVICE

SAP NS2
NATIONAL SECURITY SERVICES
CLOUD

Now, let us help you.
Learn more at sapns2.com/cloud

877-972-7672
info@sapns2.com
www.sapns2.com