Datasheet | PUBLIC

SAP National Security Services
A Secure Cloud for the Utility Industries

SAP NATIONAL SECURITY SERVICES

SAP National Security Services (SAP NS2) was founded to help protect and secure the mission critical operations of highly regulated organizations. As the U.S. sovereign cloud deployment arm of SAP, we provide the unique capability for customers in the utility industry to run market leading SAP applications without having to sacrifice security, innovation, or cost. Our team of local, credentialed experts provide the highest levels of security and compliance, deliver world class innovation, and protect critical data across all applications enterprise-wide.

THE SECURITY REGULATIONS WE DEPLOY:

- **International Traffic and Arms Regulations (ITAR)** and Export Administration Regulations (EAR) compliant solutions
- Cloud environments built to the **NIST 800-53 security standards**
- Cloud solutions designed to support mission-critical workloads and **protect BES Cyber System Information (BCSI)**

THE ROADBLOCKS: BARRIERS TO SECURELY ADOPTING CLOUD SOLUTIONS

The utility industry provides necessary amenities to many, such as water, electricity, and natural gas. When it comes to their digital transformation, utility industries are required to maintain additional security standards that extend beyond commercial cloud solutions. The keys to a secure digital transformation are:

The Speed of Innovation Paired with Heightened Security Regulations. The evolution of technology allows utility organizations to provide customers with improved services and increased reliability, but often times security gets in the way of adopting a cloud-first business model. The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) is a set of standards aimed at regulating, monitoring, and managing the security of the Bulk Electric System (BES) in North America. To ensure cloud operations are monitored properly, utility organizations need their cloud provider to understand the standards imposed upon their industry.

In-Country Solution Deployment. NERC-CIP requires BES Cyber System Information (BCSI) to be restricted to authorized personnel and prohibited from unauthorized access, as the information is vulnerable to cybersecurity attacks. One critical element that ensures enhanced security is a local support model that includes exclusively U.S. resources who have been vetted through personnel risk assessments (ie. background checks).

THE ANSWER: SAP NATIONAL SECURITY SERVICES

Infrastructure Built to Support Regulated Workloads

Our cloud infrastructure is built to protect utility organization's confidential data. We deploy solutions on highly regulated hyperscalers, such as AWS GovCloud and Azure Government, who comply with the security regulations set forth by government agencies.

Solutions Secured to Industry Standards

Our defense in depth strategy ensures preventive and detective controls are in place to protect cloud systems and data. Customers can be assured the integrity and security of NERC CIP regulated entities' BCSI, and other sensitive information, is protected.

Local Support Model to Mitigate External Risk

We support the utility's compliance to NERC CIP by ensuring all cloud resources operate according to necessary compliance levels. All supporting personnel are located within the U.S., are U.S. persons, and have been approved through background checks and security screenings.

SOLUTION OVERVIEW:

Enterprise Resource Planning:
- S/4HANA Cloud, private edition
- S/4HANA Cloud, tailored option
- S/4HANA Cloud, extended edition
- Secure HANA Cloud
- Cloud Application Services

Analytics and Innovation:
- Business Technology Platform
- SAP Analytics Cloud

Supply Chain Management:
- SAP Integrated Business Planning
- SAP Service and Asset Manager

Spend Management:
- SAP Fieldglass
- SAP Asset Intelligence Network
- SAP Business Network

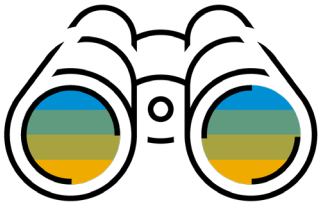
Human Capital Management:
- SAP SuccessFactors

SAP NS2'S SECURE CLOUD PORTFOLIO: THE PATHWAY TO YOUR DIGITAL TRANSFORMATION

At SAP NS2, we know that innovation fails without security. **Through our U.S. sovereign deployment model, we provide utility organizations an avenue to adopt the innovation of the cloud without compromising on security.** We strictly control how our cloud portfolio is governed, where it resides, and how its data is secured.

This control empowers utility organizations to benefit from a cloud portfolio that supports all lines of business. Our dedication to data access, data residency, and cloud sovereignty ensures financial service organizations can future proof their operations while remaining protected by their industry standards.

KEY BENEFITS:



- Industry-specific protection of mission-critical data through ITAR, EAR, FedRAMP® Moderate Controls, and NIST 800-53
- SAP NS2 experts who have deep industry knowledge of cloud business drivers and unique industry needs
- Solutions and infrastructure supported and deployed by U.S. persons on U.S. soil to ensure operations remain in country

WHY SAP NATIONAL SECURITY SERVICES: SECURE. LOCAL. SOVEREIGN.

We understand that utility organizations face different international threats and have unique compliance requirements surrounding their cloud operations. We are the solution for meeting and exceeding these challenges.

- We leverage tools such as vulnerability scanning, intrusion detection, and continuous monitoring to ensure your data stays protected with an automated security model.
- We enforce authentication and access rights to protect BES Cyber System Information (BCSI).
- Adherence to ITAR provides dedicated U.S. resources to support your cloud landscape through deep industry and regional compliance knowledge.
- We mitigate the risk of external threats by protecting system management, providing in-country deployment, and leveraging an enterprise strategy to control the data and resource access within your region.

Learn more at sapns2.com

SAP NS2 NATIONAL SECURITY SERVICES