Solution Brief | PUBLIC

SAP National Security Services
A Secure Cloud for Financial Services

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 federal civilian agencies, financial services, and U.S. defense 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:

- Adherence to **International Traffic and Arms Regulations (ITAR)** provides in-country protection of the monetary information of individuals and businesses
- Secure cloud environments built to the **NIST 800-53** Framework
- **Local support and deployment model** keeps all financial data and operations located within the U.S.

THE ROADBLOCKS: BARRIERS TO SECURELY ADOPTING CLOUD SOLUTIONS

Financial service institutions handle sensitive monetary data, therefor they are at the forefront of breaches and attacks. While commercial cloud solutions may offer the innovation needed to succeed, they often don't include the heightened security parameters needed to protect confidential financial operations. The keys to a secure digital transformation are:

Utilize Least Privilege and Need to Know Access Controls. As financial institutions constantly handle confidential banking and user information, they need to limit the amount of access points to their data. Cloud solutions must enforce role-based access controls, zero trust architecture (ZTA), and maintain Segregation of Duties and Least Privilege requirements on a need-to-know basis. Without these security controls, financial institutions open the door to cyber threats and put their customers at risk.

Solutions Built to the NIST 800-53 Security Baseline. Cyber attacks continue to grow, and financial institutions are seeking ways to protect their customer's PII and financial data. NIST 800-53 sets forth security and privacy parameters for enhanced data protection. While NIST 800-53 is not mandated for financial institutions, it has become a widely adopted framework to ensure the private sector's cloud operations are protected to the standards set in place by federal and government entities.

THE ANSWER: SAP NATIONAL SECURITY SERVICES

Stringent Data Access Controls

Your solutions are deployed with tools that enforce role-based access control (RBAC). This guarantees only credentialed individuals located and managed within the Network Operation and Support Center (NOSC) can access your data.

Solutions Built to Government Standards

Our cloud solutions meet the NIST 800-53 security framework and adhere to ITAR. Our solutions are maintained and built in a cloud environment that has been attested by a certified Third Party Assessment Organization (3PAO).

Local Deployments and Cloud Infrastructure

All solutions are deployed on local, government-attested infrastructure. This means all operations, including data backups and upgrades, are maintained within your region and data remains within the U.S., both in transit and at rest.

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

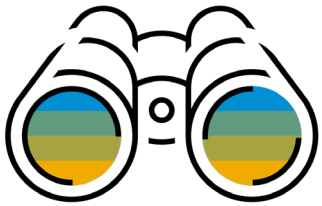
Human Capital Management:
- SAP SuccessFactors

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 financial service 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 financial 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 and NIST 800-53
- SAP NS2 experts who have deep industry knowledge of cloud business drivers and unique industry needs
- In-country operations through local deployment, infrastructure, and data residency practices

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

We understand that financial 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 under an automated security model.
- Adherence to ITAR provides dedicated U.S. resources to support your cloud landscape through deep industry and regional compliance knowledge.
- Adherence to NIST 800-53 provides a standardized model of protecting cloud solutions and sensitive financial data.
- We mitigate the risk of 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