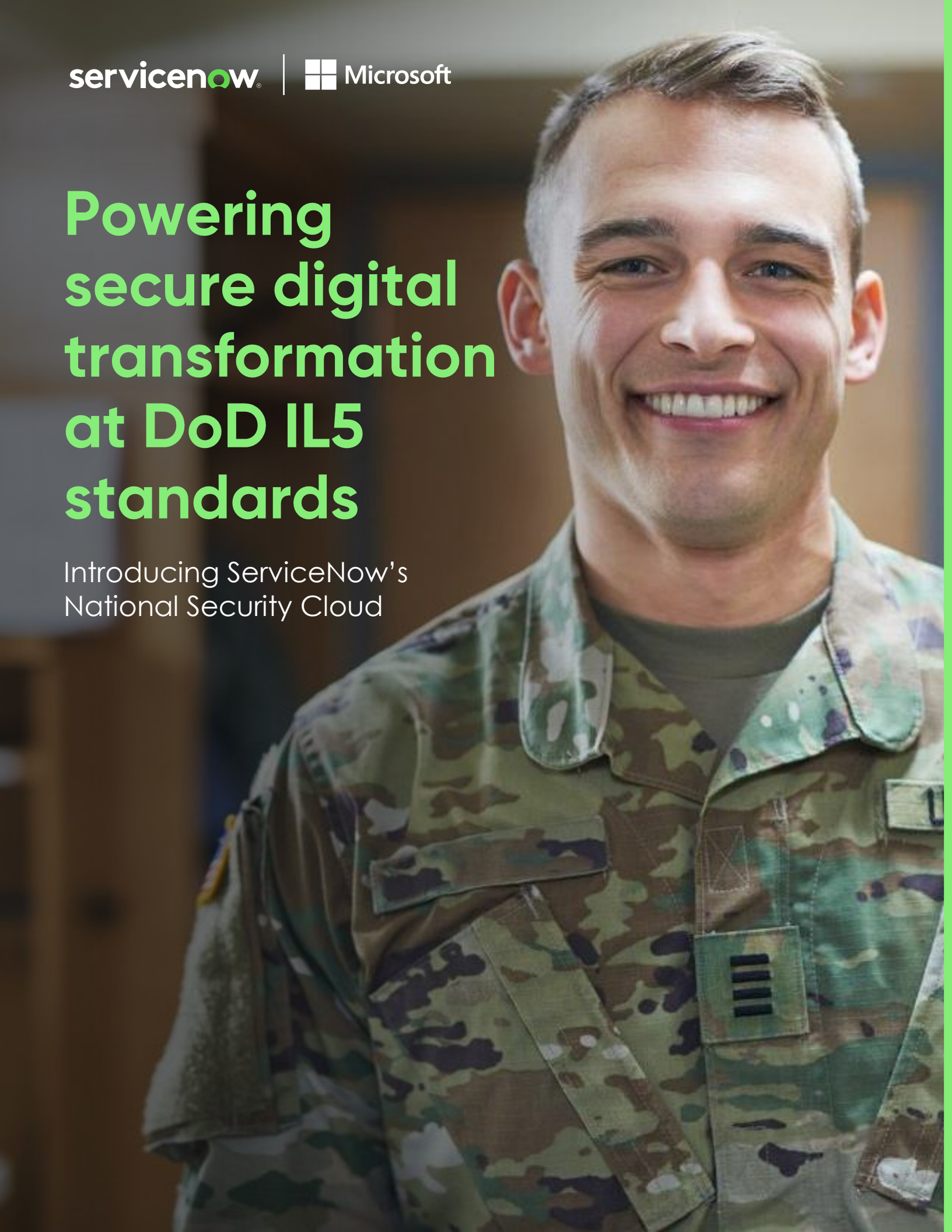
servicenow | Microsoft

Powering secure digital transformation at DoD IL5 standards

Introducing ServiceNow's National Security Cloud



Adopting cloud computing services is a priority for the Department of Defense (DoD)—a push that has been underway for more than a decade.

Its cloud-first strategy aims to reduce government spending on information technology (IT) infrastructure, such as reducing the reliance on agency-owned and operated data centers for compute and storage—and to capitalize on the other advantages that cloud solutions bring.

Every service line and DoD agency is at a different phase of this journey. Many are still self-hosting cloud environments on-premises, however embracing a cloud-first approach going forward is critical to maintain lower total cost of ownership (TCO) and high levels of availability and service for warfighters.

Cloud technology has advanced tremendously over the last five years, offering stronger security controls and providing broader capabilities that are essential to driving your mission forward. Finding the right cloud provider is critical—especially when it comes to national security data.

You need a partner that not only checks off the right compliance boxes, but also can enable your broader digital transformation goals.

That's why ServiceNow launched **National Security Cloud (NSC).** Built on Microsoft Azure Government, NSC powers compliant digital transformation in a secure **Impact Level 5 (IL5)** environment exclusively for DoD and related federal agencies.

For years, our Government Community Cloud (GCC) has helped U.S. government agencies transform the way they work. But intelligence and military agencies faced restrictions in how they could use our solutions. NSC removes this roadblock, meeting a higher level of compliance required for national security data.

Agencies can access the full power of the Now Platform®, while meeting stringent guidelines to protect national security workloads. NSC has been assessed and verified against the DoD IL5 standard to meet the most extensive security measures available for national security-level data. We expect NSC to be available for customer use in the second half of 2022.

With ServiceNow's NSC, you get a software as a service (SaaS) platform that addresses IL5 compliance, while realizing hard cost savings. Our broad range of SaaS solutions help you transform your agency's work environment—connecting your teams and systems on one platform, so they can work with greater efficiency to achieve their mission.

National Security Cloud accelerates your mission and drives cost savings

The federal government is investing in digital transformation, but it isn't easy to drive change.

ServiceNow's cloud-based SaaS solutions address some of the biggest operational challenges facing government today. We make government work better by connecting people, functions, and systems across its organization at greater speed and agility with lower cost and risk. With the Now Platform, agencies can integrate everything on a single platform, digitize workflows across systems of record, and power innovation with low-code apps.

- Extending use cases for the Non-classified Internet Protocol Router Network (NIPRNet) before moving to the more costly Secret Internet Protocol Router Network (SIPRNet)
- Enabling your people to work from home longer
- Improving talent acquisition, retention, and onboarding with more modern workplace experiences and processes
- Moving faster to adopt a broader range of workplace apps that address niche challenges, such as safely helping people return to work

Even if you're already using ServiceNow, NSC elevates your experience.

Moving to NSC from self-hosted ServiceNow	Moving to NSC from a third-party environment	Moving to the NSC from GCC
The introduction of NSC alleviates the downsides of self-hosting. Maximize the value of the Now Platform, while reducing the work it takes to maintain it. Improve service levels, reduce the risk of downtime, and take the work of maintaining your instance off your in-house resources.	If you are using a third-party hosting environment to achieve IL5 certification levels, you can still gain significant operational benefits from switching to NSC. Get more from your investment in the Now Platform, while improving availability and service levels with a true IL5-certified SaaS offering.	GCC is still a strong, supported option for those who need to meet IL4 data certification levels. However, shifting to NSC from GCC can enhance security and compliance, with additional controls for your ServiceNow instance, and extend the benefits to more workflows and data.

In this paper, we detail how NSC powers complaint digital transformation in government with:

1. Compliant engineering
2. Improved risk mitigation and cost savings
3. Embedded security

1 Engineered for compliance

Technology—and the data that supports it—is more powerful than ever before. However, data is also increasingly valuable to cyber criminals and foreign adversaries. The key is to build infrastructure that makes use of data while keeping it safe.

This means that every detail matters in the way SaaS providers build and secure their infrastructure to handle, manage, store, access, or transfer data. Any mishandling of information can have major ramifications—from losing citizen trust to risking national security. Understanding precisely how your cloud environment keeps your data protected and compliant, and the type of data it can process, is crucial.

What are the key differences between ServiceNow's GCC and NSC?

Until now, GCC was ServiceNow's standard offering for federal agencies. Certified to store and process Impact Level 4 (IL4) data, GCC can accommodate controlled unclassified information (CUI) for U.S. federal agencies, including the DoD. We will continue to maintain the secure environment it provides.

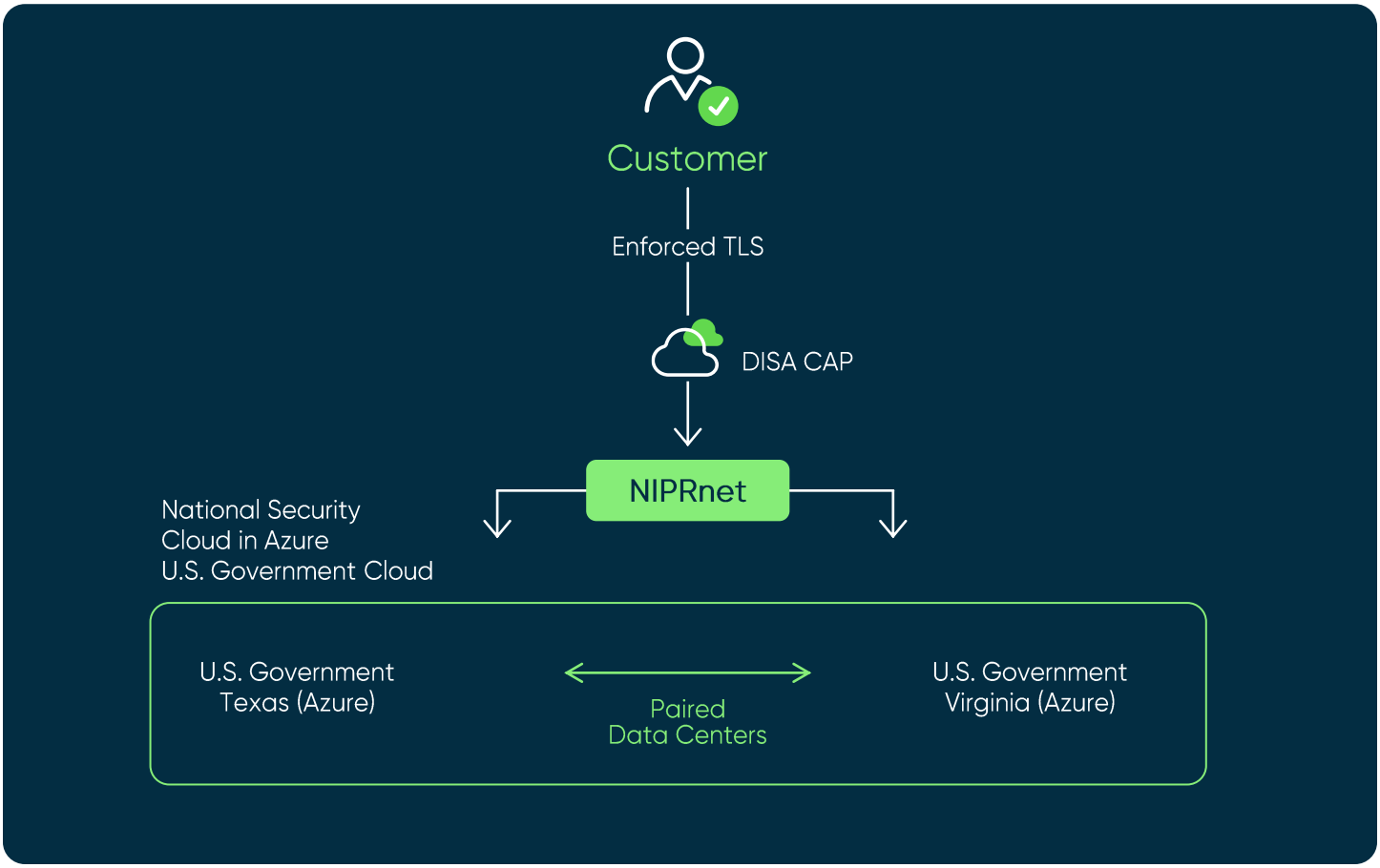
While GCC and NSC meet many of the same stringent requirements, NSC provides isolated data centers and additional security controls for agencies that require IL5 compliance to protect National Security Systems (NSS) data.

IL2	High-IL4	High-IL5
326 minimum controls	421 minimum controls	430 minimum controls
Equivalent to FedRAMP Moderate	Accommodates Controlled Unclassified Information (CUI) (e.g. FOUO)	Accommodates CUI & National Security Systems (NSS)
	• Government Community Cloud (GCC) is hosted in dedicated ServiceNow data centers • FedRAMP High baseline	• National Security Cloud (NSC) leverages hosting in Azure Government data centers • Federal government only

NSC is built to keep your data in an isolated environment

ServiceNow software is deployed on Azure Government infrastructure in the form of virtual machines. The virtual machines and software running within them are owned and operated by ServiceNow. The hypervisor and supporting infrastructure layers below it are owned and operated by Microsoft Azure Government. These hypervisors and virtual machines are not shared with any other Azure Government customers.

The illustration below shows the main points of the logical architecture.



NSC's data centers are physically isolated and separated from our commercial cloud data centers, and are reserved exclusively for DoD and related federal agencies. With NSC, customer instances (database and applications) are hosted in a pair of redundant data centers located within the U.S. Our paired data centers provide resilience and ensure data is highly available, consistent with the approach in our standard commercial offering.

Customer instances are owned and operated solely by ServiceNow. Customers always retain ownership and control of the data they store within those instances.

Data storage and processing on U.S. soil

Our NSC solution combines technology from ServiceNow and Azure, with customers' ServiceNow instances and associated services hosted exclusively in Azure Government data centers located within the U.S. All of this ensures that all customer data is stored and processed in-country, including data associated with common services, such as email and encryption key management.

Strict access controls

Another key difference between GCC and NSC is how customers access their instance. With NSC, all customers must access their instance via an established Cloud Access Point (CAP) connection to the NIPRNet. This CAP connection is provisioned by the CNS team who works directly with the customer and the Defense Information Systems Agency (DISA).

A culture of compliance

While solid controls are essential for a compliant environment, it's important not to assess them in isolation. As you evaluate cloud providers, it's equally important to consider the provider's broader reputation, experience, capabilities, and culture of compliance.

ServiceNow has mature security and compliance procedures, in-house engineering, and developer capabilities, and is rigorously audited by independent third-party companies and government bodies to prove compliance with various global and regional standards.

A comprehensive list of ServiceNow's existing certifications and attestations can be found in the Compliance section on our Trust site.

Learn more

2 Improved risk mitigation and cost savings

DoD agencies are under constant pressure to tightly manage budgets and risks. ServiceNow works with you to identify where cost savings could be realized and adjust the risk needle to your comfort zone.

For those agencies that are used to on-premises, self-hosted environments, migrating to an off-premises cloud is a big leap. But the leap comes with advantages—reducing the time, resources, risks, and costs involved in maintaining your own environment.

While it can be difficult to justify the upfront investment, consider the long-term savings related to:

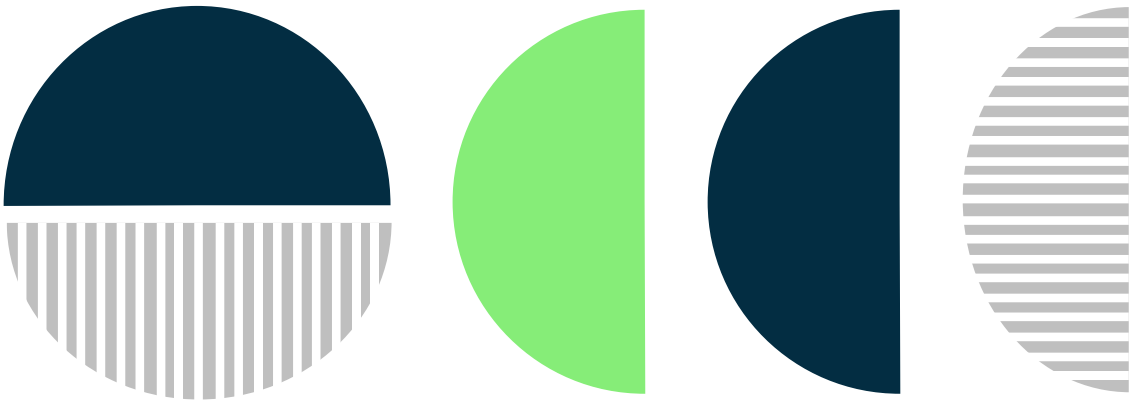
- Annual upgrades
- Internal labor costs
- Hardware costs
- External hosting partners
- Staying on NIPRNet longer, without having to move to SIPRNet

Expertly maintained environment

NSC takes some of the pressure off in-house resources that are stretched thin by escalating demands. ServiceNow takes over many of the routine maintenance responsibilities, helping you:

- Reduce the risk of downtime; ServiceNow guarantees you'll have more reliable service and more uptime on the cloud.
- Reduce the time and risks involved in upgrade issues; ServiceNow maintains your instance.
- Reduce data loss risk; ServiceNow's redundant data centers improve data resilience.

Your organization will have quick, easy access to the full suite of ServiceNow solutions. In addition, the partnership between ServiceNow and Azure Government enables seamless integration with Microsoft Office products, such as Office 365 and Microsoft Teams.



Dedicated support from in-country personnel

NSC is supported by a dedicated team of personnel who are available on a 24/7 basis. Each member of the team is a U.S. resident, located on U.S. soil. This team features subject matter experts in critical topics:

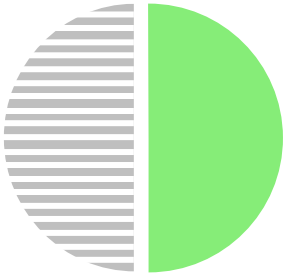
- Administration
- Automation
- Integrations
- Performance
- Platform technology
- Service management

Protecting access to data during the support process

Access to ServiceNow infrastructure within NSC is only possible by authorized ServiceNow personnel from a secure, non-persistent virtual desktop environment (VDE) hosted in the U.S. and connecting to NSC environment over secure, encrypted connections. Rigorous authentication checks must be passed to access the VDE.

Limiting access to ServiceNow personnel

ServiceNow will provide all support for NSC. We maintain a deep relationship and partnership with Microsoft and will liaise with Microsoft's support team on your behalf if necessary. Only ServiceNow personnel have access to the ServiceNow instances and customer data.



3 Embedded security

As cyber threats increase in frequency, severity, and sophistication, DoD agencies must do everything in their power to vigorously protect data. Cybersecurity is gaining a growing share of the DoD's attention and budget—lawmakers appropriated $2 billion for the Cybersecurity and Infrastructure Security Agency's 2021 budget.

NSC's secure cloud environment gives agencies greater consistency and control over protecting their critical information across the board. NSC offers strong safeguards for federal contract information and reduces the time it takes to identify and resolve associated threats.

Extra security controls

GCC and NSC environments are both assessed by U.S. FedRAMP against 421 FedRAMP High controls. NSC meets nine additional security controls required for NSS data.

Data encryption

Your data will always remain encrypted—preventing unauthorized parties from being able to read or understand your data.

NSC provides Federal Information Processing Standard (FIPS)-validated cryptography throughout the entire Azure environment for both data in-transit and data at-rest.

NSC customers also benefit from the additional protection of data-at-rest by Azure's encrypted storage, which employs SSE-CMK (Server-Side Encryption, Customer-Managed Key). This uses AES 256-bit encryption for the Key Encryption Key (known as Envelope Encryption). The keys are protected and managed by ServiceNow in a dedicated Azure Key Vault hosted within NSC data centers.

Built-in security enables you to do more with AI and automation

Under ServiceNow's GCC, security constraints inhibited some of our DoD customers from using certain product features. By investing in the additional security layers offered through NSC, those roadblocks are removed so you have the flexibility to adopt the full range of ServiceNow solutions and features to accelerate your digital transformation goals.

NSC will continuously evolve to maintain the highest security standards. ServiceNow listens to and collaborates with customers every day to innovate and sharpen available tools and processes that meet the highest security levels.

Build the future of government on National Security Cloud

The public sector is changing. Agencies understand they can't step into the future relying on the old, siloed processes and legacy systems that slow down work. You shouldn't have to choose between digital transformation and compliance.

The right cloud environment makes government more resilient, flexible, and responsive—all while keeping security at the forefront.

NSC, built on Microsoft Azure, puts innovation and security hand-in-hand. Our security-first approach gives you the ability to achieve your goals while maintaining compliance.

Learn more

servicenow | Microsoft