DELIVERING SECURE, SCALABLE, AND COMPLIANT CLOUD SERVICES

servicenow™

START >

Security & Assurance

Data Security

Security Architecture

Platform Security

Operations & Availability

Global Operations

Availability & Performance

Privacy & Compliance

Privacy

Compliance Certifications

Compliance Resources

Trust – Built Upon a Secure, Scalable, and Compliant Cloud

OVERVIEW

Instilling the utmost confidence in our ability to prevent and mitigate security threats, protect your data, and help you comply with a growing number of global mandates is our top priority. To this end, we have made significant investments in technology, processes, and expertise to ensure that our cloud services meet the most stringent of standards for security, availability, scalability, privacy, and compliance.

This ebook is designed to provide you with detailed information around how our cloud services adhere to these standards.

SECURITY & ASSURANCE

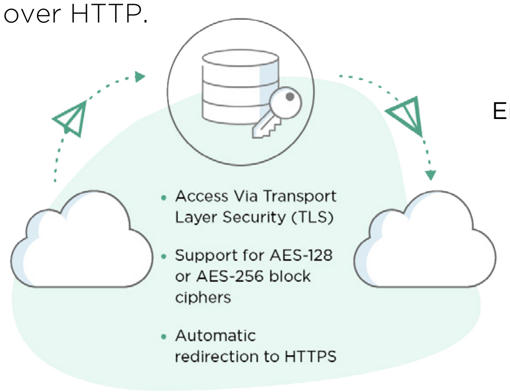
Your data security is paramount to us. We've engineered our cloud services, the infrastructure that supports it, our data encryption techniques, and security threat response processes to ensure that your data is protected and secure at all times.

Data Security

Encryption in Flight

As a customer, browser-based sessions to your ServiceNow cloud instance(s) are encrypted over the internet via Transport Layer Security (TLS) using AES-128 or AES-256 block ciphers. These ciphers are subject to the browser versions in use and may be influenced by your Internet proxy infrastructure.

You can also force specific cipher suites via your own browser or proxy if desired. All end-user access to a ServiceNow instance is always automatically redirected to HTTPS if attempted over HTTP.



• Access Via Transport Layer Security (TLS)
• Support for AES-128 or AES-256 block ciphers
• Automatic redirection to HTTPS

ENCRYPTION IN FLIGHT

Integration Encryption

We can apply encryption to integrations, such as LDAP and Web Services, as well as commonly used file transfer methods.

In the case of an LDAPS over SSL connection, you can conveniently store certificates for specific LDAP servers within a ServiceNow instance for use in signing instance-bound Web Service requests. We also support certificate-based mutual Web Services security authentication with external endpoints for all ServiceNow instances.

Data can be securely transferred to your ServiceNow instances using pre-defined file transfer integration methods. You can also use clear text protocols such as FTP or HTTP to transfer data or support specific tasks, such as an approval or status request.

< PREVIOUS

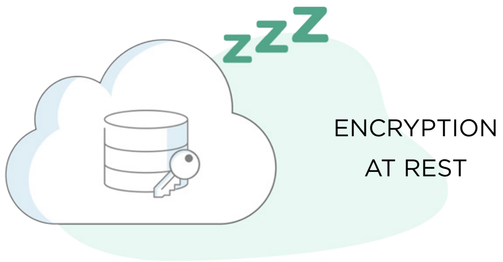
NEXT >

Security & Assurance
Data Security
Security Architecture
Platform Security
Operations & Availability
Global Operations
Availability & Performance
Privacy & Compliance
Privacy
Compliance Certifications
Compliance Resources

Email Encryption

Email encryption allows you to protect sensitive messages and comply with privacy regulations. We support opportunistic Transport Layer Security for email sent or received by a ServiceNow instance.

Our customers benefit from email encryption when they take advantage of the Now Platform to automate processes. Encrypted emails are automatically generated to support specific tasks, such as an approval or status request.



Column-Level Encryption

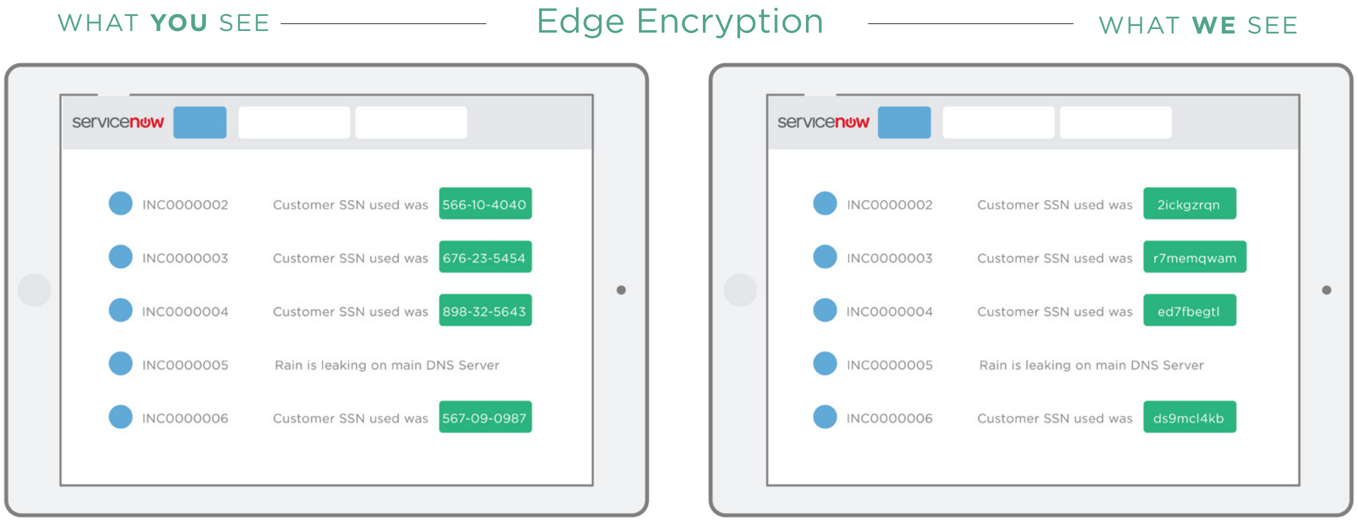
We simplify data security at the application level by giving you the option to perform column-level encryption on fields and attachments. This feature is available to all our cloud services as well as custom-built applications developed on the Now Platform.

We support AES-128, AES-256, and 3DES encryption algorithms, and apply your choice to encrypt data. To mitigate the possible compromise of encrypted customer data, we re-encrypt (wrap) your keys with a secondary key. In some cases, data stored in fields and attachments that is encrypted cannot be searched for or reported on.

Edge Encryption

The ServiceNow Edge Encryption application provides you with advanced data protection capabilities. It lets you perform data encryption using encryption keys that are stored and managed on premises. All encryption takes place inside your network through a proxy application that functions like a Cloud Access Security Broker (CASB).

With Edge Encryption, unencrypted target data is never stored in your ServiceNow instance. It provides you with the capability for automatic key rotation. It supports tokenization and substitution of data, such as credit card or social security numbers, to match standard data structures.



INC0000002	Customer SSN used was	566-10-4040
INC0000003	Customer SSN used was	676-23-5454
INC0000004	Customer SSN used was	898-32-5643
INC0000005	Rain is leaking on main DNS Server	
INC0000006	Customer SSN used was	567-09-0987

INC0000002	Customer SSN used was	2ickgzrqn
INC0000003	Customer SSN used was	r7memqwam
INC0000004	Customer SSN used was	ed7fbegtl
INC0000005	Rain is leaking on main DNS Server	
INC0000006	Customer SSN used was	ds9mcl4kb

< PREVIOUS

NEXT >

Security & Assurance
Data Security
Security Architecture
Platform Security
Operations & Availability
Global Operations
Availability & Performance
Privacy & Compliance
Privacy
Compliance Certifications
Compliance Resources

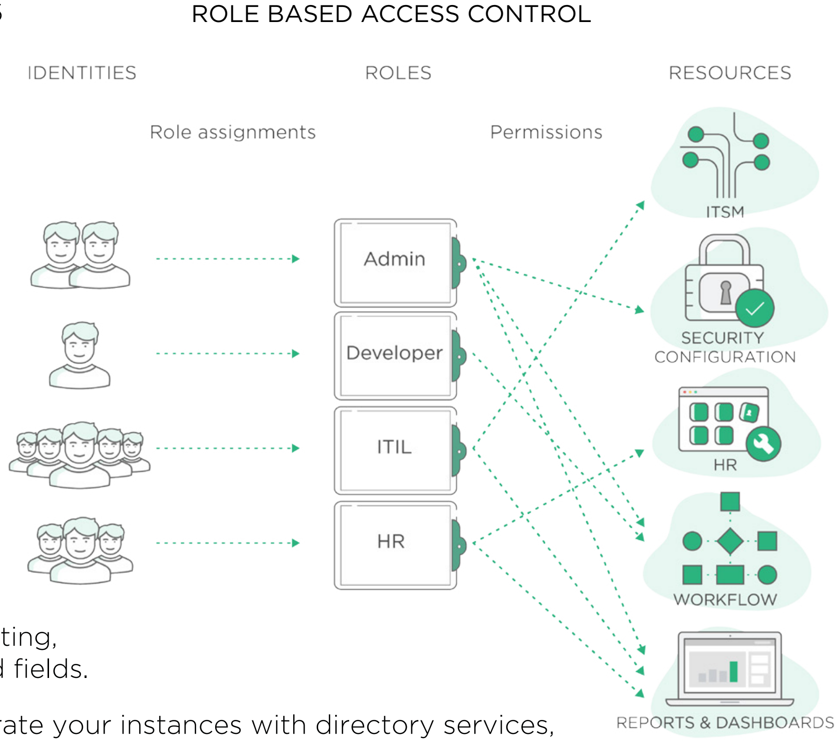
Full-Disk Encryption

Everything inside the co-location spaces are owned, operated, and managed by ServiceNow. This includes the management of hard drives and server hardware. All hard drives are sanitized prior to leaving our private cages (per NIST 800-88 guidelines) which ensures your data is appropriately handled and protected. You can choose to further mitigate data exposure caused by the loss or theft of storage devices with AES-256 full-disk encryption of your data at rest. Full-disk encryption is available at additional cost.

Access Control

You have full control of entitlements granted to each of your end users in a ServiceNow instance. This includes a built-in Role Based Access Control (RBAC) mechanism for creating user, group, and role objects. This makes it easy for you to assign access to applications and data within your instances.

Access Control Rules and Lists (ACLs) in conjunction with RBAC let you control access to entire tables, records, or fields. Several out-of-the box ACLs are included with your ServiceNow instance. You also have the ability to define your own ACLs to suit your needs. The ACLs control individual entitlements around creating, reading, writing, and deleting tables, records, and fields.



To help manage role assignments, you can integrate your instances with directory services, such as LDAP and Active Directory. This lets you leverage existing users and groups as well as easily manage users and access within your ServiceNow instances.

Information Classification

A single data classification is applied to all customer data we host. We do not inspect or monitor the data. As our customer, you apply access controls to restrict access within your instances based on your requirements and needs, in accordance with your data classification policies.

Data Retention

As a ServiceNow customer, you decide what information is to be stored, how it is to be used, and how long it is retained. We do not delete or modify your data and only process data in accordance with our contractual obligations and your configuration of your instance(s). We keep 28 days of backup. When you delete data from a ServiceNow instance, the deletion will take 28 days to be cycled out of a backup.

< PREVIOUS
NEXT >

Security & Assurance
Data Security
Security Architecture
Platform Security
Operations & Availability
Global Operations
Availability & Performance
Privacy & Compliance
Privacy
Compliance Certifications
Compliance Resources

Media Disposal

All your data is hosted on solid-state or mechanical disks within our co-location spaces. No tapes or other forms of removable media are used to provide the service, including for backups.

When functional storage devices reach their end-of-life or get reassigned to new customers, they are shredded based on guidance from the U.S. National Institute of Standards and Technology (NIST).

Data Return and Destruction

Throughout the lifetime of your subscription, your data can be directly exported from the ServiceNow instance. This can be via the user interface, through integrations, or by using other ServiceNow components. We return all your data in an SQL dump format at the end of a contract. All hosted backed-up data is automatically deleted and overwritten 45 days from the end of a contract.

Secure Data Handling

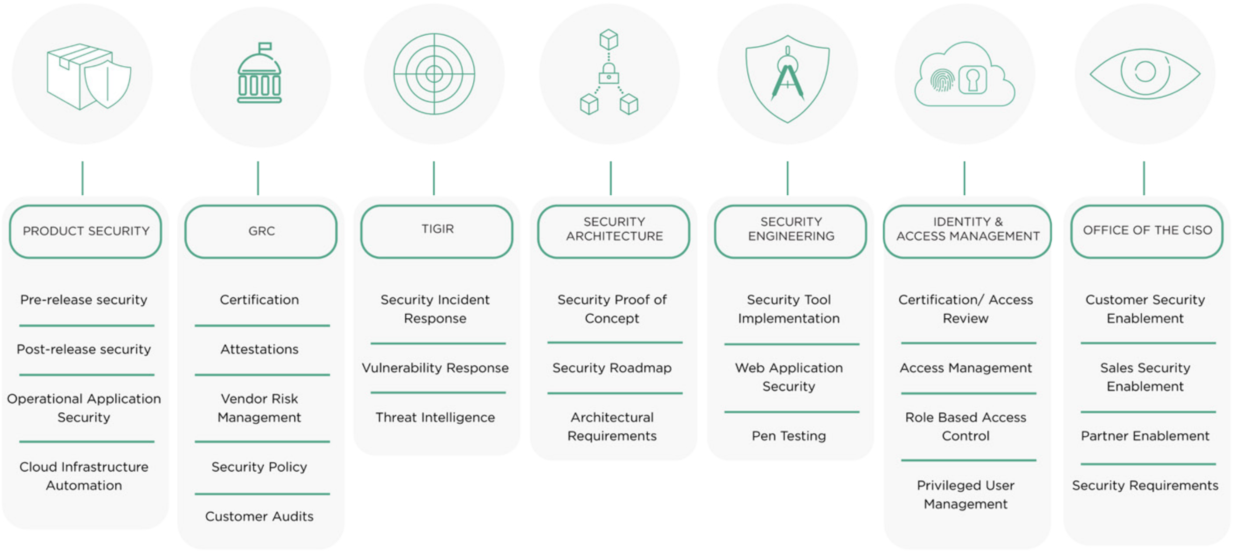
We follow the principle of least privileges to ensure that our operators have only the access necessary to perform their job. Additionally, access to our production environment is protected using multi-factor authentication and encrypted VPNs.

We have also implemented capabilities to protect against insider threats and data exfiltration. ServiceNow has a program called Controlled Access. It ensures that access to customer instances and data is logged and monitored, and that sufficient preventative controls are in place to protect customer data.

Security Architecture

Global Security Team

The ServiceNow global security team is focused on protecting the confidentiality, integrity, privacy, and availability of the data and the services we deliver. It performs the functions listed in the diagram below.



PRODUCT SECURITY	GRC	TIGIR	SECURITY ARCHITECTURE	SECURITY ENGINEERING	IDENTITY & ACCESS MANAGEMENT	OFFICE OF THE CISO
Pre-release security	Certification	Security Incident Response	Security Proof of Concept	Security Tool Implementation	Certification/ Access Review	Customer Security Enablement
Post-release security	Attestations	Vulnerability Response	Security Roadmap	Web Application Security	Access Management	Sales Security Enablement
Operational Application Security	Vendor Risk Management	Threat Intelligence	Architectural Requirements	Pen Testing	Role Based Access Control	Partner Enablement
Cloud Infrastructure Automation	Security Policy				Privileged User Management	Security Requirements
	Customer Audits					

< PREVIOUS

NEXT >

Security & Assurance
Data Security
Security Architecture
Platform Security
Operations & Availability
Global Operations
Availability & Performance
Privacy & Compliance
Privacy
Compliance Certifications
Compliance Resources

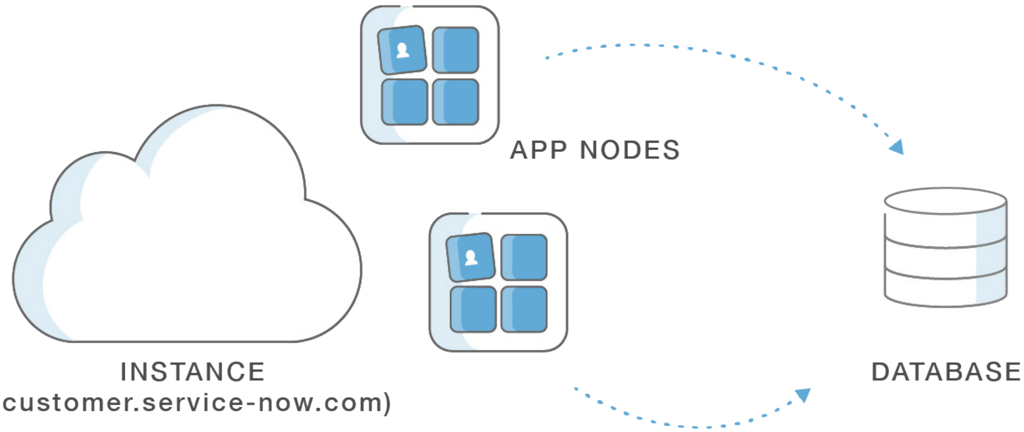
Physical Security

Physical security for the ServiceNow Nonstop Cloud begins with the global co-location data centers at which the service is hosted. The ServiceNow data centers are highly secure facilities with 24x7x365 security guards, CCTV, multiple levels of entry controls, and strict procedures for physically entering the facility. Within each data center, all ServiceNow equipment is stored in one or more dedicated, anonymous ServiceNow co-location spaces. The cages are further protected behind biometric access controlled doors. And all ServiceNow data center providers must be either ISO/IEC 27001:2013 accredited and/ or produce regular SSAE 16 Type 2 attestations.

Cloud Security

As a customer, your instanced is hosted in our SaaS environment. We refer to it as “private” because the environment is dedicated to only hosting our subscription service and no other public cloud-hosting capabilities are used to deliver the service. Also your instance is logically separated from all other tenants in our cloud environment using our multi-instance architecture.

LOGICALLY SINGLE TENANT ARCHITECTURE



< PREVIOUS
NEXT >

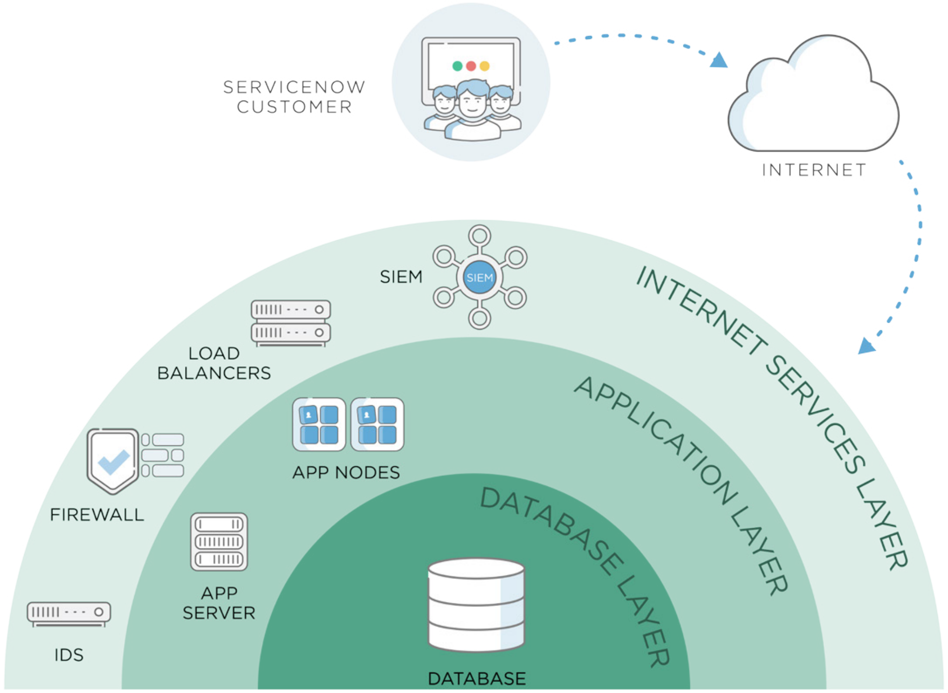
Security & Assurance
Data Security
Security Architecture
Platform Security
Operations & Availability
Global Operations
Availability & Performance
Privacy & Compliance
Privacy
Compliance Certifications
Compliance Resources

Logical Security

To protect the instances and data within the ServiceNow Nonstop Cloud, we have implemented specific logical security zones. These zones are logically separated and protected using logical access controls. The three primary zones are as follows:

- Internet Services Layer: The first zone of the architecture includes network routers, switches, load balancers with integrated network firewalls, and intrusion detection systems. These devices are deployed in a fully redundant configuration to provide the highest possible availability in the event of a failure.
- Application layer: The second zone isolates the application servers, installed in a discrete network segment inaccessible from the Internet. The servers in this zone host the application nodes for each of your ServiceNow instances. They serve as the termination point for all inbound requests from users of those instances.
- Database layer: The third zone contains the database servers that have host-based firewalls. In our multi-instance architecture, each database server runs one or more unique database processes assigned to a customer instance. Each database server runs multiple database daemons (services). One of these exists for every instance. These services only have access to a single set of database tables used solely for a particular instance.

LAYERED SECURITY MODEL



< PREVIOUS
NEXT >

Security & Assurance
Data Security
Security Architecture
Platform Security
Operations & Availability
Global Operations
Availability & Performance
Privacy & Compliance
Privacy
Compliance Certifications
Compliance Resources

Host Security

Protecting the hosts and servers in our production environment is essential for security. The protection of the host starts with the use of a hardened open source operating system that is regularly patched using automated configuration management.

Comprehensive vulnerability response processes scan all hosts daily and they are patched regularly to meet compliance mandates.

DDoS Protection

ServiceNow takes the threat of Distributed Denial of Service (DDoS) very seriously and has deployed a multi-tiered defense system that continually monitors for attacks and mitigates them. DDoS attack traffic is identified and discarded at the edge of our cloud. This allows customers to maintain access to their instances even during an attack.

In addition to the on-network defenses, we have contracted with a third-party provider to provide DDoS mitigation services in the event on-network defenses are overwhelmed.

Platform Security

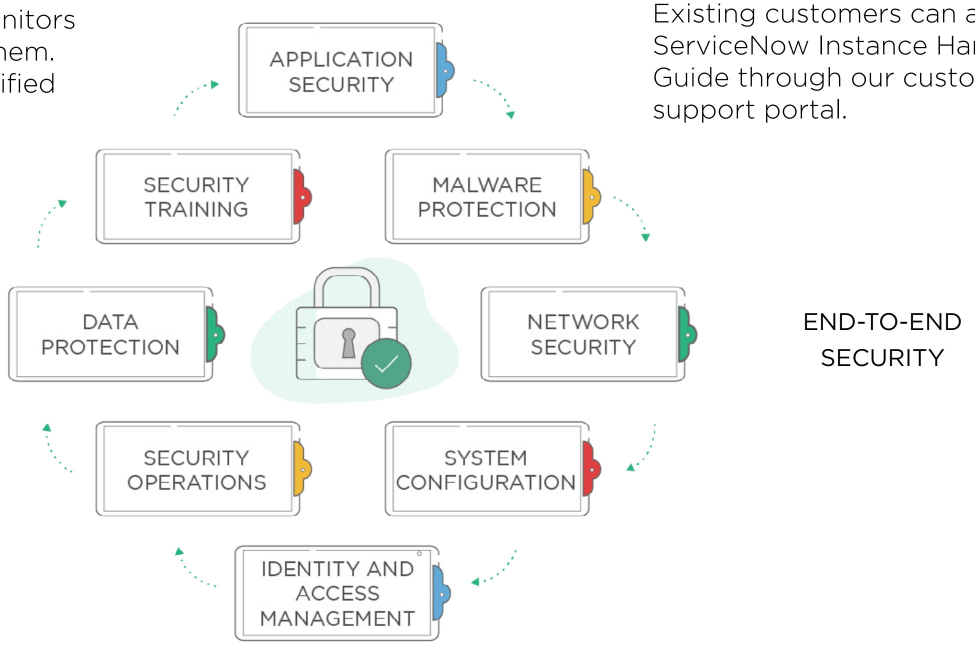
Secure by Default

We add new security properties to each release of the Now Platform and provide specific recommendations about how to enable these properties within the ServiceNow Instance Hardening Guide. As a customer, you benefit from the services we provide that support application security, malware protection, network security, system configuration, Identity and Access Management (IAM), security response, and data protection.

A high security plugin provides advanced security options that can be enabled in all new ServiceNow instances. The plugin enforces the default deny access mode and enables access control rules. It provides elevated access functionality and security-related roles for a customer's instance administrators.

The plugin also includes out-of-the-box security-related properties. For example, you can set restrictions on the nature and types of attachments that can be uploaded into the instance, how those attachments behave when downloaded, and other hardening attributes.

Existing customers can access the ServiceNow Instance Hardening Guide through our customer support portal.



< PREVIOUS
NEXT >

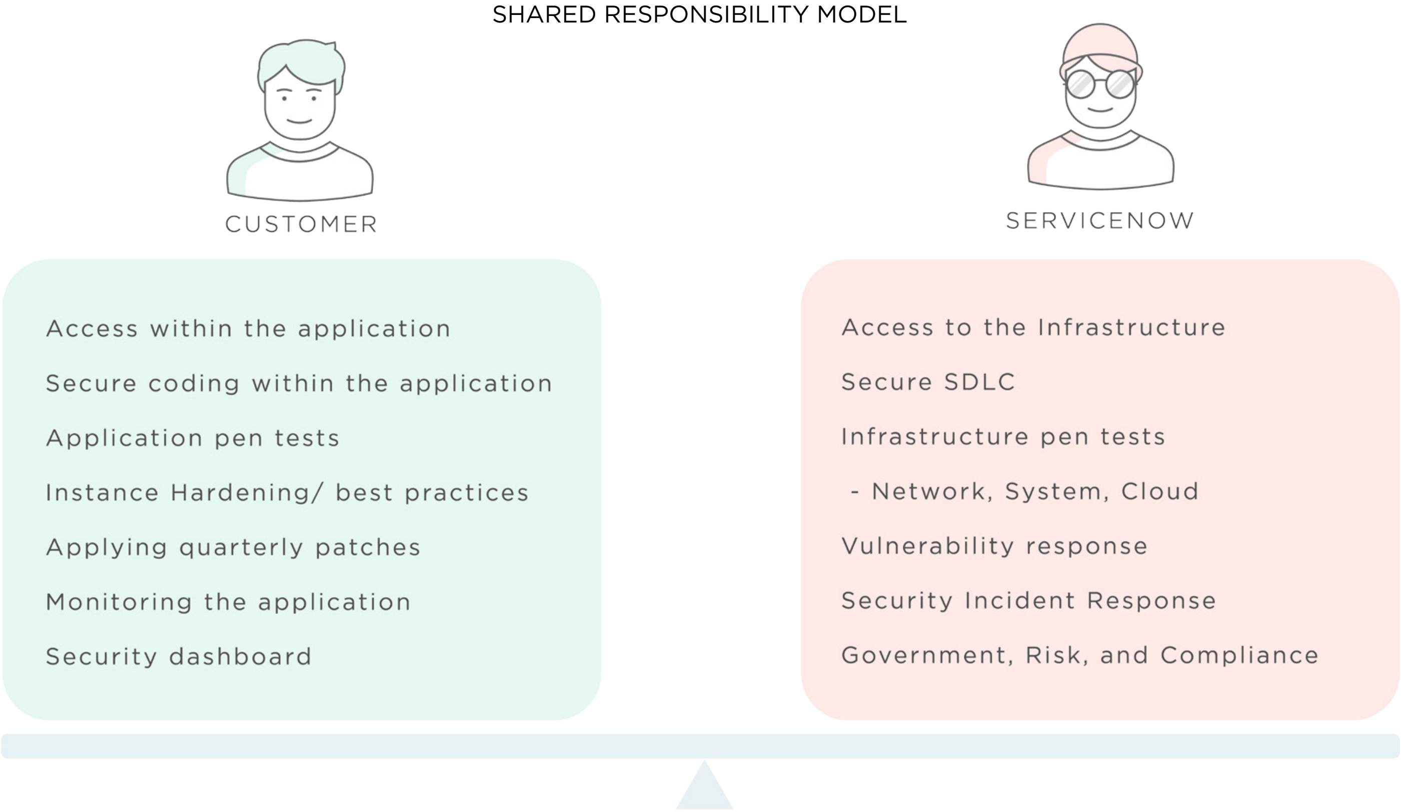
Security & Assurance
Data Security
Security Architecture
Platform Security
Operations & Availability
Global Operations
Availability & Performance
Privacy & Compliance
Privacy
Compliance Certifications
Compliance Resources

Customer-Controlled Security

As a ServiceNow customer, you have control over the security of your instance and your data within the ServiceNow cloud services. As discussed previously, you can choose from several data-at-rest encryption options, manage application-level role based access controls, and authentication mechanisms. As a customer, you are also contractually permitted to conduct an application-level penetration test against your sub-production instance every year.

You also have the ability to control specific security settings within the instance that enables you to harden the application and platform settings to meet your unique security needs.

Existing customers can learn more about customer-controlled security by accessing the ServiceNow Instance Hardening Guide through our customer support portal.



SHARED RESPONSIBILITY MODEL

CUSTOMER

- Access within the application
- Secure coding within the application
- Application pen tests
- Instance Hardening/ best practices
- Applying quarterly patches
- Monitoring the application
- Security dashboard

SERVICENOW

- Access to the Infrastructure
- Secure SDLC
- Infrastructure pen tests
  - Network, System, Cloud
- Vulnerability response
- Security Incident Response
- Government, Risk, and Compliance

< PREVIOUS

NEXT >

Security & Assurance
Data Security
Security Architecture
Platform Security
Operations & Availability
Global Operations
Availability & Performance
Privacy & Compliance
Privacy
Compliance Certifications
Compliance Resources

Identity Management

Users of a ServiceNow instance require an identity within the database, regardless of authentication mechanism. This helps support a variety of capabilities within the cloud service, including role-based access and transaction/ configuration item (CI) association.

To facilitate this, your instances support both manual creation of user identities as well as automated mechanisms like Active Directory, LDAP, and external identity providers (IDPs). The instance synchronizes users, their group memberships, and the group objects themselves. You can incorporate as few or as many user attributes as you deem necessary, although passwords cannot be synchronized. .

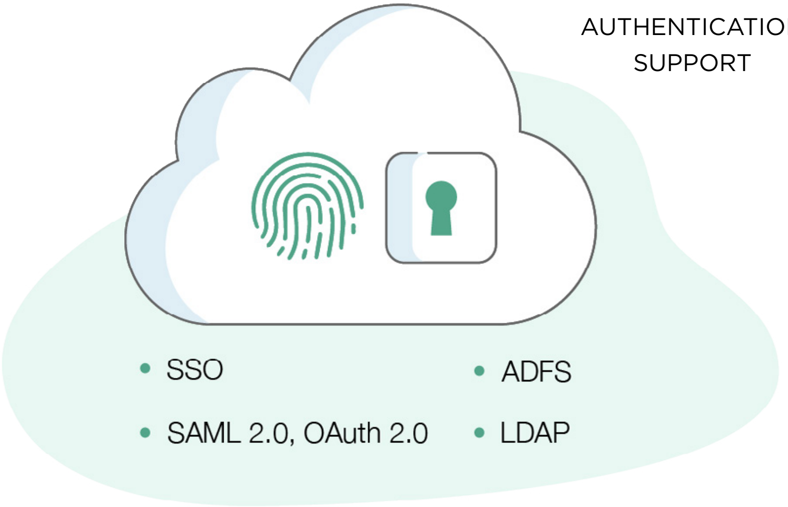
Customers may also use the ServiceNow Management, Instrumentation, and Discovery (MID) server component for LDAP synchronization. The MID server can be installed inside your internal network to access your directory servers. This eliminates the need to allow the ServiceNow instances through your perimeter and firewall for server access.

Authentication

To give you the most flexibility, ServiceNow supports several authentication options. This allows you to use several methods within your instance. Your instance supports “native” or local authentication (for example, when user credentials are stored in the instance) and OAuth 2.0 authentication (such as for external client authentication), as well as multi-factor authentication mechanisms.

The ServiceNow SAML plugin supports SSO-based authentication through a variety of SAML 2.0-compliant identity providers. This include Active Directory Federation Services (ADFS) as well as third-party identify providers, such as Ping, SecureAuth, SailPoint, Okta, or others that are compliant with the SAML 2.0 standard. If you have already implemented your own SAML-compliant IDP or leverage a third-party service, you can use the same capability for your ServiceNow instance.

LDAP authentication enables customers to use their own LDAP-compliant directory services such as Active Directory. A directory needs to be accessible to the relevant ServiceNow instance, as often these are located behind a firewall or other perimeter control. As part of the LDAP integration, passwords are not stored or transferred back to your ServiceNow instance.



< PREVIOUS
NEXT >

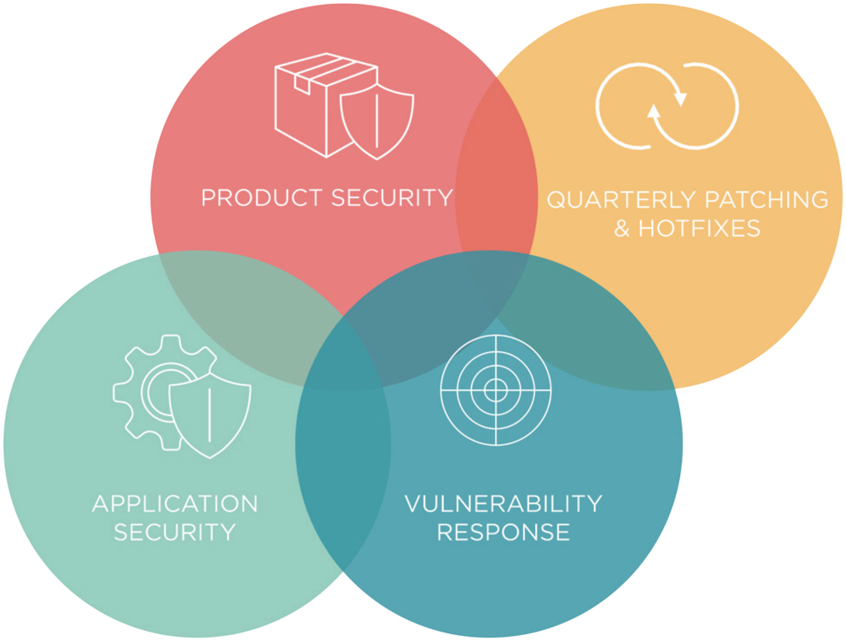
Security & Assurance
Data Security
Security Architecture
Platform Security
Operations & Availability
Global Operations
Availability & Performance
Privacy & Compliance
Privacy
Compliance Certifications
Compliance Resources

Software Development Lifecycle Security

Security is an embedded component of the Software Development Lifecycle (SDLC) at ServiceNow. We use an Agile development process that includes validation steps run by an independent product security team. Developers and other relevant personnel are regularly trained on web application security, through a variety of methods, including classroom-based training. This includes, but is not limited to, training from organizations such as the Open Web Application Security Project (OWASP).

Dedicated security engineers who are part of the ServiceNow security department are embedded into our overall SDLC. These team members support secure development by:

- Managing the various internal and external testing programs
- Managing vulnerability response across the cloud environment
- Managing the quarterly patching program and hotfixes as needed
- Performing assessments of internal ServiceNow services and instances that support our business
- Performing architectural reviews for new security features
- Curating educational material on security



SERVICENOW'S SDLC

< PREVIOUS
NEXT >

Security & Assurance
Data Security
Security Architecture
Platform Security
Operations & Availability
Global Operations
Availability & Performance
Privacy & Compliance
Privacy
Compliance Certifications
Compliance Resources

Application Security Testing

Application security testing occurs throughout the lifecycle. During development, code for the release is subject to continuous ongoing testing and review using methods that include commercial and in-house automated toolsets. Manual testing, peer code reviews, and Dynamic Application Security Testing (DAST) are also part of our development testing process. These processes and tools are used to test the patches and hotfixes applicable to each supported version.

For added assurance, a third party tests every major release using a grey box methodology. Findings from this test are addressed and re-tested as part of the release process. This ensures an objective assessment of the cloud service before it is released to customers.

Customer Penetration Testing

Existing customers may perform an annual application penetration test using a documented process. ServiceNow works with customers to pre-approve the testing schedule. This allows us to continue to monitor and differentiate potential real attacks from authorized customer activity.

We require that our customers share their results with us. Confirmed customer findings help contribute to the collective security of the ServiceNow environment and enable us to continuously improve our security posture.

Customer penetration testing represents a significant number of tests annually. If these tests produce genuine, confirmed vulnerabilities, we remediate those in accordance with our vulnerability response criteria. We document what has been remediated in each major version, patch, and hot fix within the release notes.

Existing customers can access additional information around the penetration testing process through the customer support portal.

Patch Management

There are two major releases of the Now Platform each year. We also produce patches and hotfixes throughout the supported lifetime of a major release.

We automatically schedule patch installations on a per-customer and per-instance basis. Our multi-instance model allows customers to request alternate dates for the patches to be applied. Hotfixes are also applied at a customer's discretion unless deemed mandatory for availability or security reasons.

Your instance of ServiceNow can continue to be used during a major release upgrade, patch, or hotfix installation.

We perform continuous and automated scanning of our infrastructure to identify vulnerabilities or patch discrepancies. The findings are first reviewed by our expert staff to ensure that the appropriate level of priority is assigned, taking into factors such as relevant mitigating controls. Published or identified vulnerabilities that initially seem significant may in reality represent a lower risk to our environment, as with all published vulnerabilities.

We also use the Advanced High Availability architecture to transfer customers' production instances between data centers when we perform maintenance, such as patching, which further minimizes the impact to availability.

< PREVIOUS
NEXT >

Security & Assurance
Data Security
Security Architecture
Platform Security
Operations & Availability
Global Operations
Availability & Performance
Privacy & Compliance
Privacy
Compliance Certifications
Compliance Resources

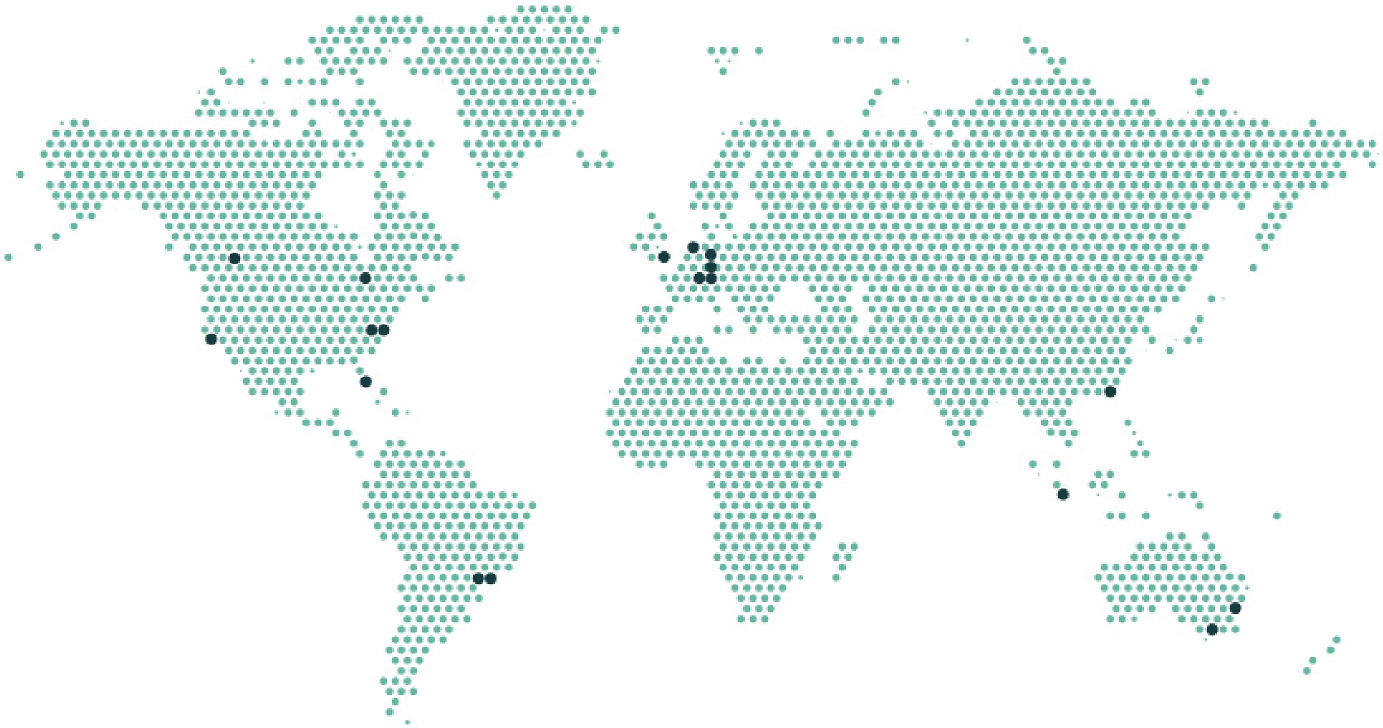
OPERATIONS AND AVAILABILITY

We believe that cloud services must always be on. Our unique, multi-instance architecture lets you configure your cloud services and perform upgrades on your own schedule. And our advanced, high availability infrastructure provides instance redundancy between data center clusters in your chosen geography. It scales to meet the needs of even the largest global enterprises.

Global Operations

Global Infrastructure

The ServiceNow Nonstop Cloud was designed to support the availability and scalability requirements of Global 2000 enterprises. We operate nine data center pairs for a total of 18 data centers to meet our customers' location and data sovereignty needs. Each data center pair operates in an active-active mode providing highly performant and available instances for our customers. Our data centers span five continents: Asia, Australia, Europe, North America, and South America.



< PREVIOUS
NEXT >

Security & Assurance

Data Security

Security Architecture

Platform Security

Operations & Availability

Global Operations

Availability & Performance

Privacy & Compliance

Privacy

Compliance Certifications

Compliance Resources

At ServiceNow, operational excellence is a top priority. To meet this goal, we have invested in the following:

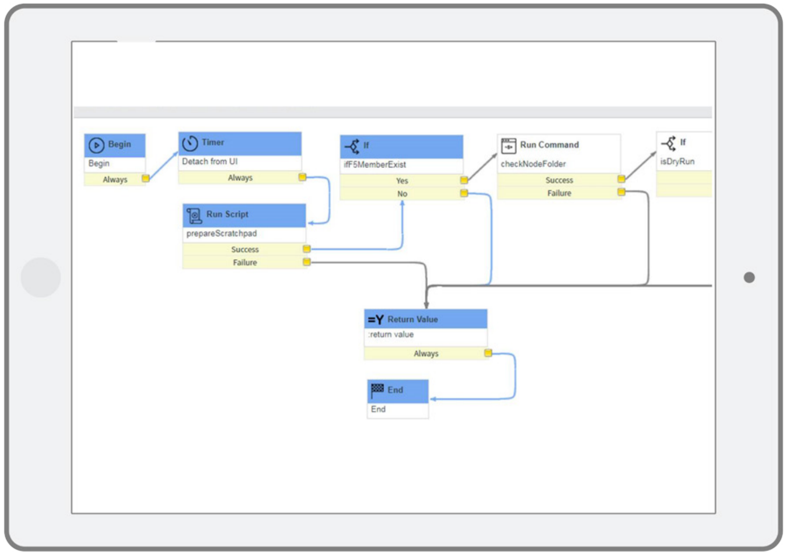
- Best-of-breed data center sites built and designed to support our customers' high-availability requirements. These sites meet the highest standards for reliable power, fire suppression, and physical security
- Redundant devices and power across all network and server infrastructure
- Secure infrastructure with redundant firewalls, intrusion detection systems (IDS), load balancers, and Distributed Denial of Service (DDoS) protection in every location
- ServiceNow-owned and operated equipment, with all locations staffed by full-time employees

Automation

We use the power and flexibility of the Now Platform to automate the provisioning, monitoring and scaling of our Nonstop Cloud. Customers on the Now Platform in the Nonstop Cloud benefit from the ability to leverage the same operational capabilities that we use in-house for their own enterprise automation.

We use the Now Platform to automate many tasks for customers on the Nonstop Cloud. We provision new instances using the ServiceNow workflow capabilities. We can create a byte-for-byte copy of a customer instance (a process we call "cloning") for use as a test or development environment and add capacity to customer instances—all using automation.

We can ensure the availability of our customer instances using our advanced high availability automation that moves customer instances between the pairs of data centers in each geography. Our operations teams use both DevOps and ITILv3 practices as well as the ServiceNow Incident, Problem, Change, Knowledge, Notify and custom-written business applications extensively.



AUTOMATED INSTANCE PROVISIONING

< PREVIOUS

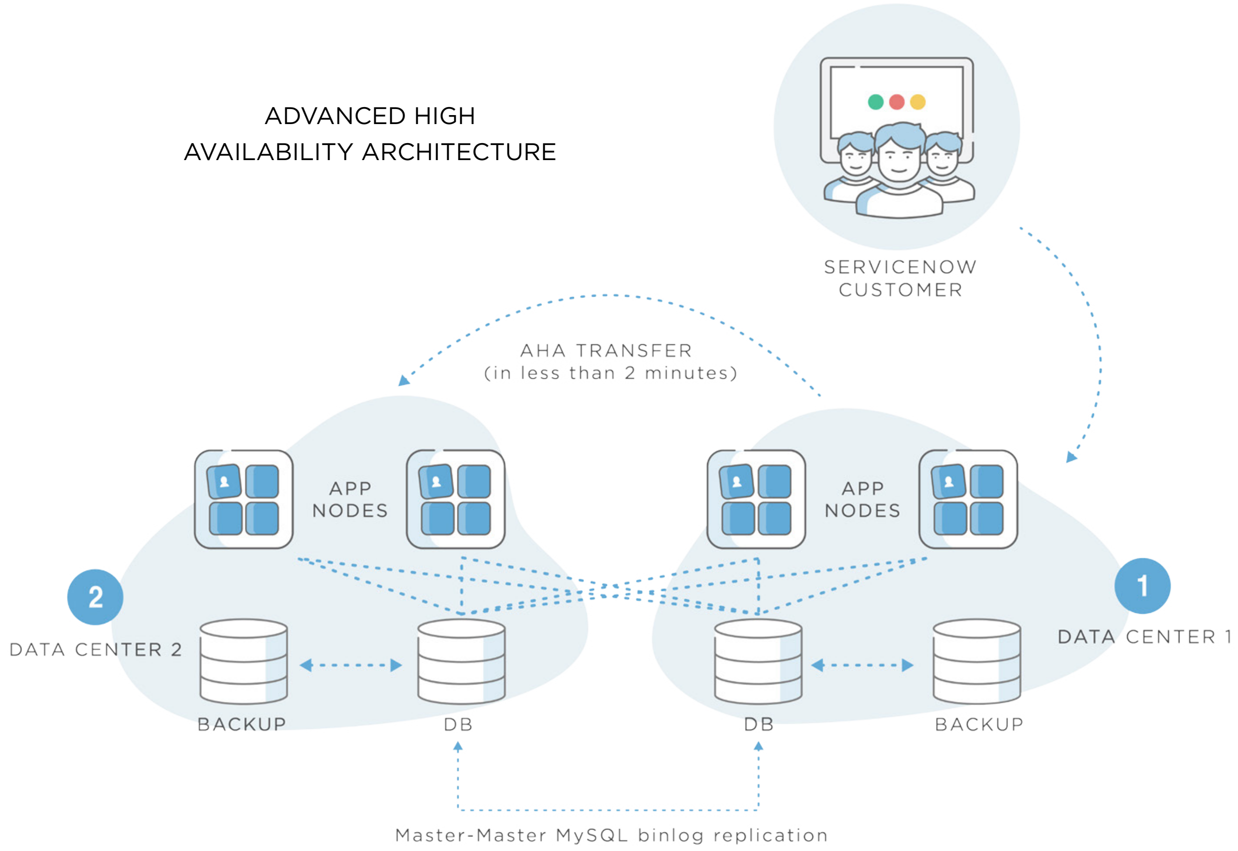
NEXT >

Security & Assurance
Data Security
Security Architecture
Platform Security
Operations & Availability
Global Operations
Availability & Performance
Privacy & Compliance
Privacy
Compliance Certifications
Compliance Resources

Business Continuity and Disaster Recovery

ServiceNow's production cloud environment is architected to host customer instances from regionally-located and geographically dispersed data center pairs that operate in an active-active mode. Instance data is replicated in near real-time between the two data center pairs. In the event of an operational fault, failure, outage or attack, customer traffic can be quickly rerouted using our Advanced High Availability (AHA) capability to ensure you maintain access to your instances and data.

For disasters that could impact an entire data center, ServiceNow maintains comprehensive disaster recovery, business continuity, and information system contingency plans that cover our production environments.



< PREVIOUS
NEXT >

Security & Assurance
Data Security
Security Architecture
Platform Security
Operations & Availability
Global Operations
Availability & Performance
Privacy & Compliance
Privacy
Compliance Certifications
Compliance Resources

Availability and Performance

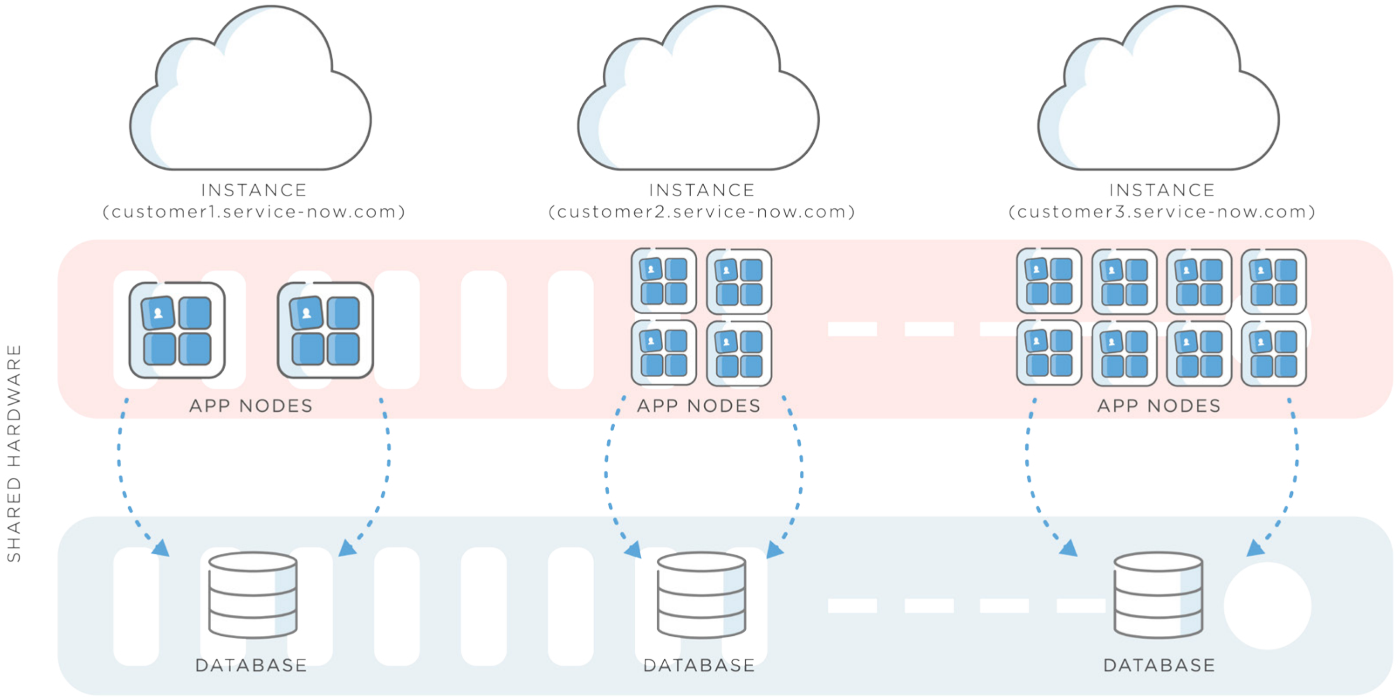
Multi-Instance Architecture

The ServiceNow Nonstop Cloud is deployed on an advanced, multi-instance architecture that separates a customer's application nodes and database. This means there is no co-mingling of customer data.

We deploy instances on a per-customer basis, allowing the multi-instance cloud to scale horizontally to meet each customer's performance needs.

Unlike in a multi-tenant environment, each instance runs its own application logic and database processes. This means your instance does not have to be on the same version or upgraded at the same time as other customers' instances. You can choose to upgrade your instances on a schedule that best meets your enterprise's needs and compliance requirements.

PHYSICALLY MULTI-INSTANCE ARCHITECTURE WITH HORIZONTAL SCALING AND LOAD BALANCING



< PREVIOUS
NEXT >

Security & Assurance
Data Security
Security Architecture
Platform Security
Operations & Availability
Global Operations
Availability & Performance
Privacy & Compliance
Privacy
Compliance Certifications
Compliance Resources

Availability

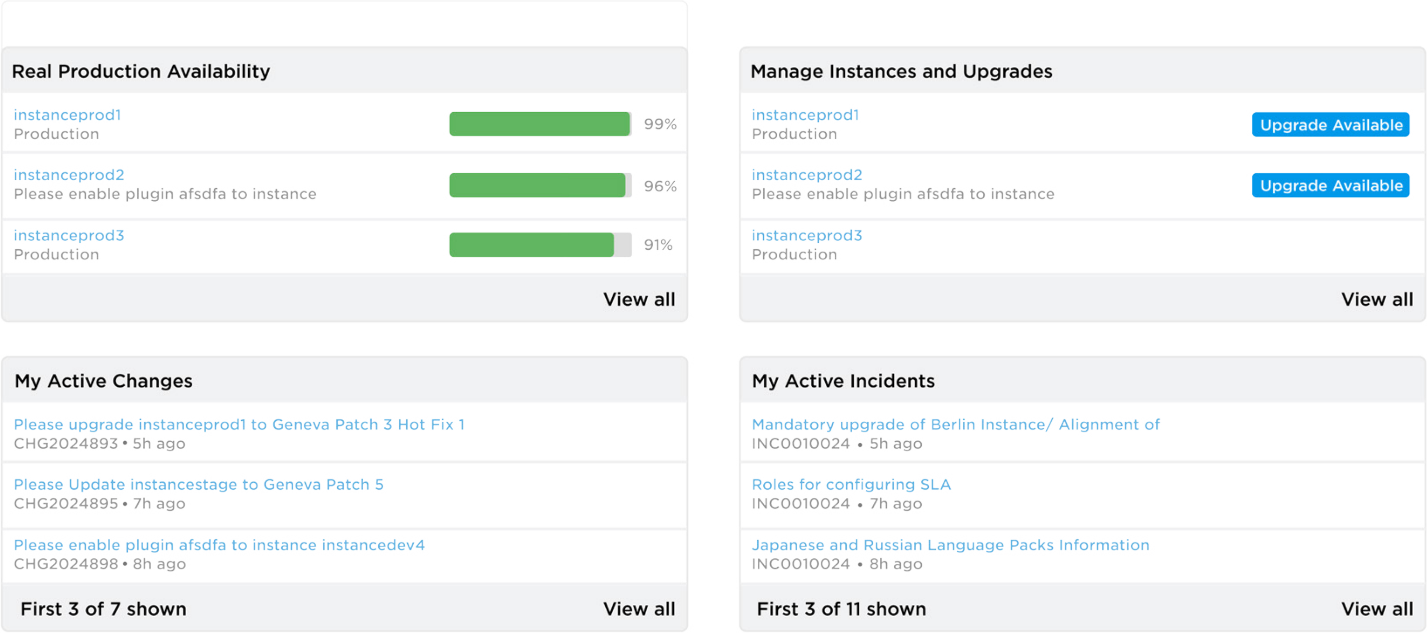
The ServiceNow Nonstop Cloud aims to be always operational for our customers. No vacation, no extended upgrade or maintenance windows, no single points of failure. We focus on near-perfect availability with redundancy built in to every layer of our cloud, including redundant devices and power across all network and server infrastructure. There is no downtime necessary for upgrades.

We provide the industry's only Real Availability Dashboard that shows availability of all your instances running in the cloud. Real Availability is the true measure of customer availability by looking at every incident that results in a customer outage (a Priority 1 or P1 incident).

Performance

Our Nonstop Cloud scales to meet the needs of the largest Global 2000 enterprises and aims to be always operational for our customers. We have tens of thousands of customer instances operating globally in our data center regions. Each of our customer instances leverages our multi-instance architecture to perform an aggregate of tens of billions of full page transactions every month. Customers using the ServiceNow Configuration Management Database (CMDB) as the single system of record have scaled their CMDBs to manage tens of millions of configuration items (CIs).

REAL AVAILABILITY AND TRANSPARENCY



Real Production Availability

instanceprod1
Production — 99%

instanceprod2
Please enable plugin afsdfa to instance — 96%

instanceprod3
Production — 91%

View all

Manage Instances and Upgrades

instanceprod1
Production — Upgrade Available

instanceprod2
Please enable plugin afsdfa to instance — Upgrade Available

instanceprod3
Production

View all

My Active Changes

Please upgrade instanceprod1 to Geneva Patch 3 Hot Fix 1
CHG2024893 • 5h ago

Please Update instancestage to Geneva Patch 5
CHG2024895 • 7h ago

Please enable plugin afsdfa to instance instancedev4
CHG2024898 • 8h ago

First 3 of 7 shown — View all

My Active Incidents

Mandatory upgrade of Berlin Instance/ Alignment of
INC0010024 • 5h ago

Roles for configuring SLA
INC0010024 • 7h ago

Japanese and Russian Language Packs Information
INC0010024 • 8h ago

First 3 of 11 shown — View all

< PREVIOUS
NEXT >

Security & Assurance
Data Security
Security Architecture
Platform Security
Operations & Availability
Global Operations
Availability & Performance
Privacy & Compliance
Privacy
Compliance Certifications
Compliance Resources

PRIVACY AND COMPLIANCE

As a customer, you always maintain ownership and control over the data you entrust to the ServiceNow Nonstop Cloud. Our approach to privacy is founded upon our commitment to giving you full control over the use, collection, and distribution of your customer data.

We continue to adhere to one of the broadest portfolios of industry standards that include ISO 27001, ISO/IEC 27018, SSAE SOC 1 Type 2 and SOC 2 Type, and the FedRAMP. And we remain committed to complying with new digital privacy and safety mandates as they continue to evolve.

PRIVACY

GDPR

The new General Data Protection Regulation (GDPR) helps protect and ensure the privacy rights of European Union (EU) citizens and residents. The GDPR establishes global privacy requirements governing how you manage and protect personal data of EU citizens and residents while respecting individual choice—regardless of where data is sent, processed, or stored.

At ServiceNow, we believe that the GDPR is an important step toward strengthening data protection laws across the European Union and enabling individual privacy rights. This is why ServiceNow is committed to being GDPR-compliant across our cloud services when enforcement begins on May 25, 2018. Read more about our commitment to complying with the GDPR.

Privacy Policy

As a ServiceNow customer, we understand that you are entrusting us with your data. This is why we take a principled approach to privacy, security, and compliance, with strong commitments to ensuring you can trust the cloud services you rely on.

Our Privacy Statement explains our privacy practices, including what personal data we collect and how we use it.

Our commitment to data privacy and security is further highlighted by a comprehensive set of third-party compliance certifications and attestations.

Privacy Shield Framework

We comply with the EU-U.S. Privacy Shield Framework and the Swiss–U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Economic Area and Switzerland to the United States.

You can view a description of how we comply with the Privacy Shield Principles in our Privacy Shield Policy. To learn more about the Privacy Shield Framework and the scope of our participation, visit the U.S. Department of Commerce website.

Cookies and Other Technologies

Our Cookies Policy applies to the ServiceNow Website and describes the information that we collect by using automated information-gathering tools, such as cookies and web beacons.

ServiceNow uses cookies to collect certain information, enhance your browsing experience, and make your interactions with our Website more meaningful. For example, we may use cookies to determine whether you have visited our Website before. It informs us about site features that you are interested in, allowing us to better tailor our Website content to your needs.

You can learn more about our cookies policy here.

< PREVIOUS

NEXT >

Security & Assurance
Data Security
Security Architecture
Platform Security
Operations & Availability
Global Operations
Availability & Performance
Privacy & Compliance
Privacy
Compliance Certifications
Compliance Resources

COMPLIANCE CERTIFICATIONS

Regional Compliance

We recognize that your compliance and certification requirements vary by the regions in which you operate. Our certification efforts span a comprehensive set of compliance requirements that apply to numerous industries and geographic regions. Our regional certifications include the following:

Certification Name	Geography
ISO 27001	International
ISO 27018	International
SSAE 16 SOC 1 Type 2 & SOC 2 Type 2	United States
FedRAMP Moderate JAB ATO	United States
Pink Verify	International
EU Privacy Shield	European Union
Multi-Tier Cloud Security Standard	Singapore
Australian Signals Directorate	Australia

ISO 27001

ISO 27001 is a security management standard that specifies security management best practices and controls based on ISO/IEC 27002:2013 best practice guide. As an ISO/IEC 27001-certified organization there is a high level of integration between the ISO/IEC 27002:2013 code of practice and the ServiceNow Information Security Management System (ISMS). The ISO 27001 certification validates that ServiceNow:

- Systematically evaluates our information security risks, taking into account factors including the impact of company threats and vulnerabilities
- Designed and implemented comprehensive information security controls and risk management practices to address company and architecture security risks
- Adopted a continuous risk management process to ensure that the appropriate information security controls are in place to meet an evolving threat landscape and risks

ServiceNow has been an ISO 27001-certified organization since 2012.

ISO 27018

ISO 27018 expands upon the controls implemented in 27002 with an emphasis on the protection of personal data in the cloud.

ServiceNow became ISO 27018-certified in 2016.

SSAE 16 SOC 1 Type 2 and SOC 2 Type 2

The American Institute of Certified Public Accountants (AICPA) developed the Service Organization Control (SOC) framework that outlines controls organizations can implement or be assessed by, to protect the confidentiality and privacy of information in the cloud.

The SOC 1 controls focus on the effectiveness of

< PREVIOUS
NEXT >

Security & Assurance
Data Security
Security Architecture
Platform Security
Operations & Availability
Global Operations
Availability & Performance
Privacy & Compliance
Privacy
Compliance Certifications
Compliance Resources

internal controls that affect the financial reports of customers.

The SOC 2 evaluates controls that are relevant to security, availability, processing integrity, confidentiality, or privacy.

ServiceNow is audited annually by a third party and has maintained its SSAE 16 SOC 1 Type 2 certification since 2011 and SOC 2 Type 2 certification since 2013.

Accessibility 508

ServiceNow is committed to making our products accessible to everyone. We develop our products to adhere to Section 508 Amendment to the Rehabilitation Act of 1973 and the guidelines Web Content Accessibility Guidelines (WCAG) 2.0 Level A.

ServiceNow publishes a Voluntary Product Assessment with each release on the ServiceNow Product Documentation site.

FedRAMP Moderate Certification (for U.S. Government entities)

The U.S. Federal Risk and Authorization Management Program (FedRAMP) was established to provide a standardized approach for assessing, monitoring, and authorizing cloud computing products and services under the Federal Information Security Management Act (FISMA), and to accelerate the adoption of secure cloud solutions by federal agencies.

ServiceNow received its Moderate P-ATO in 2016.

The FedRAMP Moderate P-ATO also meets the requirements for DoD Impact Level 2.

Pink Verify

ServiceNow was the first SaaS vendor to achieve Pink Verify status on 11 ITIL processes back in 2009. ServiceNow has continuously evolved and improved its IT Service Management solutions while maintaining this industry certification.

Multi-Tier Cloud Security Singapore Standard (for Singaporean Government entities)

The Multi-Tier Cloud Security (MTCS) is an operational Singapore security management standard. It is based on ISO 27001/02 Information Security Management System (ISMS) standards that allows for Singaporean government entities to leverage ServiceNow.

ServiceNow achieved MTCS Level 3 Certification in 2016.

Australian Signals Directorate

ServiceNow is certified by the Australian Signals Directorate (ASD) and registered under the Information Security Registered Assessors Program (IRAP) as a cloud service provider suitable for Australian government organizations. The IRAP is an ASD initiative. It includes a framework for endorsing individuals from the private and public sectors who can deliver cyber security assessment services to Australian government organizations. Endorsed IRAP assessors can independently assess ICT security, suggest mitigations, and highlight residual risks.

< PREVIOUS

NEXT >

Security & Assurance
Data Security
Security Architecture
Platform Security
Operations & Availability
Global Operations
Availability & Performance
Privacy & Compliance
Privacy
Compliance Certifications
Compliance Resources

COMPLIANCE RESOURCES

ServiceNow CORE

ServiceNow CORE (Compliance Operations Readiness Evidence), hosted on the ServiceNow Community Site, brings together an extensive set of documentation that outlines how ServiceNow helps our customers address their compliance and regulatory requirements for cloud services.

Our customers can easily access the documentation they need to address their internal audit and vendor assessment requirements, as well as other regulatory requirements (e.g., FDA, ISO, and SOX), related to their use of ServiceNow.

ServiceNow CORE offers industry-specific guidance for life sciences quality management (including the IQOQ process), healthcare, higher education, and financial services industries. It constantly evolves as new documentation becomes available or additional industry-specific information is incorporated.

Compliance Questionnaire

ServiceNow uses the Standardized Information Gathering (SIG) questionnaire as a tool for risk management assessments of cybersecurity, IT, privacy, data security, and business resiliency. The SIG is an industry-standard questionnaire that allows for a broad range of different industries to quickly assess security and risk management practices at ServiceNow. It is available through ServiceNow CORE.

CSA STAR Registry

The Cloud Security Alliance (CSA) Security, Trust, and Assurance Registry (STAR) program assists customers with performing due diligence on cloud service providers. ServiceNow has completed the CSA Star Level 1: Self-Assessment and it is available through the ServiceNow CORE site.

ServiceNow is also a CSA member and contributor.

SUMMARY

Partnerships that last are built upon a foundation of trust. At ServiceNow, we strive to deliver safe and secure cloud services that you can rely on to run your business. Our state-of-the-art security infrastructure, data encryption techniques, and threat response processes ensure that your data is always protected and secure. Our advanced, high-availability infrastructure and a multi-instance architecture provides you with cloud services that are reliable, configurable, and scalable. And we remain committed to adhering to one of the broadest portfolios of industry standards, and complying with privacy and safety mandates as they continue to evolve.

< PREVIOUS
NEXT >

< PREVIOUS