Securing the Now Platform®
An overview of the ServiceNow security program
Release: Washington, DC
Document summary

ServiceNow® provides a cloud-based platform and solutions that deliver digital experiences to automate, predict, digitize, and optimize business processes and tasks across the enterprise.

ServiceNow customers gain the benefits of a common, highly standardized cloud infrastructure, while realizing the security benefits of customer-specific isolation at the application and database layers.

The ServiceNow Commercial Cloud is built on a multi-instance logically single-tenant architecture. This provisions a dedicated database for each customer instance, ensuring there is no possibility of accidental co-mingling of data.

Having a single product, platform, and support infrastructure means that ServiceNow can employ a large global security team dedicated to securing the Now Platform.

This document describes the ServiceNow security program across a number of key physical, administrative, and logical security domains. These include Advanced High Availability architecture, information lifecycle, physical security, security operations, disaster recovery/business continuity, privacy, compliance, and software development. All these domains are represented from the context of ServiceNow as both a software vendor and as an operator of a large private cloud infrastructure.

ServiceNow is proud to be a founding member of the AI Alliance, joining forces with other pioneering organizations to advance the principles of open, safe, and responsible AI (Artificial Intelligence) globally.

Please note: all information in this white paper is related to the standard Now Platform commercial environment.

For information related to other globally located ServiceNow in-country cloud offerings and how these offerings may differ, please contact your ServiceNow account representative.
# Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Document summary</strong></td>
<td>2</td>
</tr>
<tr>
<td><strong>Introduction</strong></td>
<td>6</td>
</tr>
<tr>
<td>Complementary industry documents.</td>
<td>6</td>
</tr>
<tr>
<td>The ServiceNow CORE Compliance Portal</td>
<td>6</td>
</tr>
<tr>
<td>ServiceNow Security Center (SSC)</td>
<td>7</td>
</tr>
<tr>
<td>High Security Settings plugin</td>
<td>7</td>
</tr>
<tr>
<td>AI and Generative AI</td>
<td>7</td>
</tr>
<tr>
<td>ServiceNow terminology</td>
<td>8</td>
</tr>
<tr>
<td><strong>Security responsibilities</strong></td>
<td>9</td>
</tr>
<tr>
<td>Data roles and responsibilities</td>
<td>9</td>
</tr>
<tr>
<td>The shared security model</td>
<td>9</td>
</tr>
<tr>
<td><strong>Information security governance and risk management</strong></td>
<td>10</td>
</tr>
<tr>
<td>Security frameworks</td>
<td>10</td>
</tr>
<tr>
<td>Security policy, standards, and procedures</td>
<td>10</td>
</tr>
<tr>
<td>Security management</td>
<td>10</td>
</tr>
<tr>
<td>Risk management</td>
<td>11</td>
</tr>
<tr>
<td>ServiceNow organization entitlement reviews</td>
<td>11</td>
</tr>
<tr>
<td>Human resources security</td>
<td>11</td>
</tr>
<tr>
<td><strong>Compliance</strong></td>
<td>12</td>
</tr>
<tr>
<td>Why certification matters</td>
<td>12</td>
</tr>
<tr>
<td>Regulatory and industry compliance</td>
<td>12</td>
</tr>
<tr>
<td><strong>Physical and logical architecture</strong></td>
<td>13</td>
</tr>
<tr>
<td>Overview of physical architecture</td>
<td>13</td>
</tr>
<tr>
<td>Global data center pairs</td>
<td>13</td>
</tr>
<tr>
<td>Data sovereignty</td>
<td>14</td>
</tr>
<tr>
<td>Data center physical security and environmental controls</td>
<td>14</td>
</tr>
<tr>
<td>Logical access to ServiceNow infrastructure</td>
<td>16</td>
</tr>
<tr>
<td>Overview of logical architecture</td>
<td>17</td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td>19</td>
</tr>
<tr>
<td>Advanced High Availability (AHA) overview</td>
<td>19</td>
</tr>
<tr>
<td>Transfer and failover</td>
<td>20</td>
</tr>
<tr>
<td>Data backup and recovery</td>
<td>21</td>
</tr>
<tr>
<td>Business continuity and disaster recovery</td>
<td>21</td>
</tr>
</tbody>
</table>
Software Development Lifecycle (SDLC) ........................................... 22
Secure software development ............................................. 22
Customer application penetration testing ......................... 23

Information lifecycle and data management ...................... 25
Information classification .................................................. 25
Data retention ....................................................................... 25
Media disposal .................................................................... 25
Data return and destruction .............................................. 25

ServiceNow security operations management ..................... 26
Infrastructure vulnerability management ......................... 26
Operating system security .................................................. 26
Infrastructure and application security services ................. 26
Distributed denial of service (DDoS) ................................. 26

Vulnerability management .................................................. 27
Now Platform vulnerability management ......................... 27
Cloud infrastructure vulnerability management ................. 27

Instance integrations .......................................................... 27
Overview of instance integrations .................................. 27

Now Platform MID Server ................................................... 28
MID Server diagram ......................................................... 28
Web services integration .................................................... 28
Now Platform malware protection .................................. 29
Instance communication hierarchy ................................. 29

Accessing data ................................................................... 29
Authentication .................................................................... 29
Authorization ...................................................................... 31
ServiceNow access to customer data ............................... 32

Security logging and monitoring ...................................... 33
Logging and monitoring: Now Platform instances .......... 33
Logging and monitoring: ServiceNow security infrastructure 34
Introduction

This document provides a comprehensive overview of the physical, administrative, and technical controls ServiceNow has in place to secure the Now Platform, and how they combine to protect customer data.

Please note: all information in this white paper is related to the standard Now Platform commercial environment.

Looking for a quick answer to a specific question, check out the Cloud Security Alliance (CSA) — (CAIQ) ServiceNow SIG questionnaire which contains over 250 Q&A pairs specifically designed to assist in carrying out vendor risk assessments on cloud providers.

Complementary industry documents

The following documents are designed to be read in conjunction with this paper.

- FedRAMP customer overview
- ServiceNow security and HIPAA
- Financial services white paper
- ServiceNow security for the UK public sector

The ServiceNow CORE Compliance Portal

Watch the CORE Compliance Portal Overview Video.

Find out how to access the ServiceNow CORE Compliance Portal here.

The ServiceNow CORE Compliance Portal is a documentation library supporting customers with a need to assess ServiceNow compliance to specific regulatory requirements, and other standards.

The CORE Compliance Portal enables ServiceNow customers to quickly find documentation they need to help address their internal audit, and vendor assessment requirements related to features of the Now Platform.

The CORE Compliance Portal also includes prefilled industry standard questionnaires containing over 1,100 questions and answers specifically designed for assessing cloud providers. These documents are updated annually to provide current information regarding the services provided by ServiceNow.

Once access has been provisioned to the CORE Compliance Portal customers (and prospects under NDA) can locate these key resources to assist in evaluating ServiceNow as a vendor:

ServiceNow prefilled Industry Standard Vendor Risk Assessment Questionnaire
- Standardized Information Gathering (SIG) Questionnaire

SOC 2 Type 2 Reports from third-party auditors that validate ServiceNow security controls
- SOC 2 Type 2 Report and Bridge Letter

CORE Directory Table of Contents

- Overviews
- Corporate Information
- Information Security Policies
- ServiceNow Certifications
- ServiceNow SOC Reports
- Data Center Certifications
- Standard Pre-filled Vendor Risk Assessment Questionnaires
- Access
- Accessibility & Web Content Accessibility Guidelines
- Asset & Record Management
- Audit, Risk, Compliance, GRC
- Cloud Observability
- Data Destruction
- Disaster Recovery (DR), Business Continuity Plan (BCP), Availability
- Encryption
- Environmental, Social and Governance (ESG)
- Healthcare, HIPAA, Life Sciences
- Human Resources
- Incident Response
- Infrastructure
- Physical Security
- Privacy / GDPR
- Quality
- ServiceNow on Azure
- Software Development Lifecycle, Change Management
- Support Mapping & White Papers
- Training
- Vulnerability Management, Penetration Testing

The Now Platform is a powerful cloud application platform that enables customers to link real-time data with activities, tasks, and processes to achieve better work outcomes.
ServiceNow Security Center (SSC)

The ServiceNow Security Center (SSC) is an application with a set of tools designed to help customers easily improve the security and compliance of their Now Platform instances.

The SSC Security Hardening tool allows customers to view their compliance with the ServiceNow recommended settings as a percentage score, identify the top non-compliant hardening settings that improve compliance, and allows easy changes of the settings to strengthen their security posture.

In addition, the SSC Security Metrics tool provides over 60 different security KPIs that can be monitored, and this tool creates notification alerts to help identify potential security issues and insecure user behaviors.

High Security Settings plugin

The ServiceNow High Security Settings plugin provides advanced security options for Now Platform instances. This plugin is enabled in all new instances and cannot be disabled.

Security features enforced by the plugin include the “default deny” access mode, enablement of access control rules, along with elevated access functionality, and elevated security-related roles for customer administrators.

The High Security Settings plugin also includes a number of out-of-the-box security-related properties. Customers can access, and enable, these from a single page in their instances. For example, restrictions can be set on the nature and type of attachments that can be uploaded into the instance, how those attachments behave when downloaded, and other hardening attributes.

AI and Generative AI

ServiceNow is proud to be a founding member of the AI Alliance, joining forces with other pioneering organizations to advance the principles of open, safe, and responsible AI globally.

AI adoption and technology is moving fast and worldwide legislation is following suit. The adoption of the AI Act in the EU marks the beginning of a new AI era. The EU AI Act is the world’s first, and only, set of binding requirements to mitigate AI risks.

In the US, an executive order from President Joe Biden in 2023, requires Artificial Intelligence (AI) developers to share safety results with the US government. Other countries have developed, or are developing, regulations and laws of their own.

The Now Platform brings the power of AI to organizations — delivering all the capabilities, security, and analytics customers need to help people get work done easier, faster, and smarter. ServiceNow provides AI specific opt-in agreements for our customers, which provide assurance that the machine learning and AI features of ServiceNow products can be used with confidence.

Find more information on the ServiceNow approach to security and privacy of AI related products in Data Handling and Security in AI Products.
ServiceNow terminology

The Now Platform environment is a private enterprise cloud service wholly owned and operated by ServiceNow. This cloud service features a multi-instance architecture that delivers logical single tenancy by isolating all customers’ data from each other.

The ServiceNow cloud uses an enterprise-grade cloud architecture with dedicated database and application services for each customer instance, ensuring there is no possibility of commingling customer data, unlike a multi-tenant architecture with a shared database.

- **ServiceNow cloud**
  ServiceNow instances operate in a single, globally standardized cloud infrastructure. This is supported by a global support organization, operating to a single set of processes and tools under a common governance and compliance framework.

- **The Now Platform**
  The Now Platform is a powerful cloud application platform that enables customers to link real-time data with activities, tasks, and processes to achieve better work outcomes.

- **Instance**
  An instance is an entirely discrete single deployment of the Now Platform provided to a customer, consisting of two or more application nodes and a single database that stores all data, code, and the configuration for the instance.
Security responsibilities

Data roles and responsibilities

As the data controller, customers retain ownership of their data. Therefore, customers are responsible for meeting the privacy legislation requirements in the jurisdictions where they operate and collect personal data.

If an individual requests information directly from ServiceNow (regarding data about them that may be stored on the Now Platform), ServiceNow will always refer that individual to the data controller, the customer.

ServiceNow fulfills the role of data processor and complies with the associated obligations it entails. However, ServiceNow has no visibility of the conditions under which the data was collected by the customer, whether appropriate permission was obtained, or if the data is being used in accordance with those conditions.

Regardless of how a customer classifies data stored in their instance, the single database and shared security model of the Now Platform ensure that customer data is protected.

The shared security model

Security is a partnership between the provider and customer, both with specific responsibilities. ServiceNow provides its customers with extensive capabilities to configure their instances to meet their own security policies and requirements.

However, overall security responsibilities are shared between customers, ServiceNow, and the data center provider. The areas of responsibility are shown in the table below.

For more information about security responsibilities (with respect to customer data) please see the ServiceNow Shared Responsibility Model overview.

<table>
<thead>
<tr>
<th>Area of Responsibility</th>
<th>Customer</th>
<th>ServiceNow</th>
<th>Colocation (data center providers)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure configuration of instance</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication and authorization</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data management (classification and retention)</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data encryption at rest</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data encryption in transit</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Encryption key management</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Security logging and monitoring</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Secure SDLC processes</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Penetration testing</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Vulnerability management</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Compliance: regulatory and legal</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Employee vetting or screening</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Physical security/environment controls</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Cloud infrastructure security management</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure management</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media disposal and destruction</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup and restore</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business continuity and disaster recovery</td>
<td>●</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Information security governance and risk management

Security frameworks

The ServiceNow security framework is based on ISO/IEC 27002. As an ISO/IEC 27001 certified organization, there is a high level of integration between the ISO/IEC 27002 code of practice and the ServiceNow information security management system (ISMS).

ServiceNow has been an ISO 27001 certified organization since 2012 and is also ISO/IEC 27017, 27018, and 27701 certified.

ServiceNow provides applications within the Now Platform relating to process and service management. This includes IT service management based on the globally recognized ITIL (Information Technology Infrastructure Library) process model. ServiceNow uses this best practice methodology and its principles internally to operate and manage its private cloud environment, as well as its customer-facing support model.

By leveraging its own products, ServiceNow is able to utilize security operations, regulatory compliance, and vendor risk management, ultimately providing more secure and reliable services.

Security policy, standards, and procedures

The ServiceNow security program is described in its Information Security Management System (ISMS) and associated security policies and standards. These are reflected in a comprehensive collection of Standard Operating Procedures (SOPs) and other relevant documentation and guidance. SOPs, for example, define the actions that must be carried out in a wide variety of situations according to the overall security policy.

Examples of ServiceNow SOPs include:

- Security Incident response
- Data handling
- Secure development procedures
- Risk assessment
- Incident management, problem management, and change management
- Access entitlements and review process
- Configuration management
- Vendor risk management
- Human resources and information

These documents are assessed and updated through a managed program and are updated when significant changes occur or, at a minimum, every two years.

The above SOPs and many ServiceNow security policies can be found on the CORE Compliance portal, available to prospects (under NDA) and customers. Find out how to access CORE here.

Security management

The ServiceNow Chief Information Security Officer (CISO) reports to the Chief Information Officer (CIO) and in turn to the Chief Executive Officer (CEO). This simple organizational structure provides executive visibility and oversight regarding security and risk.

The CISO is supported by a number of domain specialist teams. These include security architecture, security engineering, security operations and threat response, application security, and audit, risk, and compliance. There are also specific teams for liaising with customers on security matters, shaping employee behavior, and creating documentation or other resources.

The roles of each of these teams, and individuals within the teams, are clearly defined and ServiceNow employs standard information security best practices in its security processes, such as separation of duties and the four-eyes principle.
Risk management

ServiceNow has defined processes and procedures for managing and assessing information system and operational security risks.

ServiceNow undergoes regular assessments to identify and assess the likelihood and impact of risks. These potential risks include unauthorized access, use, disclosure, or disruption to ServiceNow systems and customers. Risks are categorized in accordance with a formally documented procedure.

Key security, risk, and compliance stakeholders meet regularly to discuss security and risk items. Any identified risk is quickly and efficiently managed in a timely manner to safeguard the confidentiality, integrity, and accessibility of ServiceNow systems and customer data. ServiceNow executive leadership is regularly briefed on current and new security risks, as well as any potential threats that could impact ServiceNow and its customers.

ServiceNow organization entitlement reviews

ServiceNow has a dedicated Identity and Access Management (IAM) team with an active IAM entitlement program that requires frequent reassertion of entitlement along with a comprehensive review.

At a minimum, quarterly entitlement reviews are carried out to ensure that personnel have the appropriate logical and physical access rights assigned to them. This includes individuals responsible for management of the ServiceNow private cloud and physical colocation spaces. Reviews also take place when personnel change roles within ServiceNow.

A service catalog of ServiceNow roles and request types is implemented internally and is used both for new requests and reassignment of access for existing personnel. This approach mitigates potential incorrect assignment of access, which can occur when access is simply copied from one user to another.

The majority of ServiceNow personnel have no access to any systems hosting customer data, or to customer data in general.

Human resources security

Upon commencement of the employment process for all prospective candidates, ServiceNow undertakes background checks and screening. Subject to per-country restrictions, these include criminal, employment, financial, citizen status, and government watch lists. Drug testing also takes place in jurisdictions that allow it. Failure to pass these tests will result in either mandatory disqualification from the employment process, or a follow-up investigation.

As a condition of accepting employment, ServiceNow personnel are required to sign a non-disclosure agreement and review and confirm their understanding of the ServiceNow Code of Conduct and Ethics policy, along with the Acceptable Use Policy. This confirmation is recorded electronically.

Without exception, all ServiceNow personnel are required to undergo annual General Security Awareness Training (GSAT). Fulfillment of required training is measured and enforced. The content of the training varies from year to year, as different security topics, risks, threats, and requirements are identified.

Personnel whose roles may bring them into contact with customer data are also required to undertake additional training.

The lifecycle of a user within ServiceNow is controlled by standard operating procedures for the creation, modification, and deletion of user identities.

ServiceNow operates integrated HR, IT, and IAM processes built on its own products. These products operate independently for both the corporate environment and the completely separate customer cloud environment.

Access control is based on job function, using the principle of least privilege, with entitlement reviews conducted regularly.

Employees exiting ServiceNow have all access removed within a maximum period of 24 hours.
Compliance

Why certification matters

ServiceNow provides highly resilient and secure cloud-based services to customers all around the world. Ensuring that customer data is protected is always a top priority.

To demonstrate this commitment to customers, ServiceNow maintains many global and regional security and privacy certifications including the internationally recognized ISO 27001, ISO 27017, ISO 27018, and ISO 27701. A full list of security-related certifications are publicly available on the Compliance page of the ServiceNow Trust site.

In addition, ServiceNow provides transparency into its security program by providing prospects and customers with access to certifications, attestations, standard operating procedures, penetration test results, and third-party audits through the ServiceNow CORE Compliance Portal.

Find out how to access the CORE Compliance Portal here.

Regulatory and industry compliance

ServiceNow supports customers in meeting vertical-specific regulatory requirements through features of the Now Platform, organizational transparency, and a shared security responsibility model.

ServiceNow has a dedicated Cloud Assurance team responsible for a number of governance and compliance efforts across the organization, including managing the ServiceNow compliance program. This team engages across multiple functional areas within ServiceNow, including legal, finance, and procurement.

The ServiceNow legal organization engages both internal and external legal counsel to understand obligations to existing (and new) laws and statutory regulations within the jurisdictions where it operates. The finance department is responsible for ensuring that ServiceNow is compliant with relevant financial regulations, including Sarbanes Oxley (SOX), a requirement for all US public companies.

In addition, ServiceNow operates a Quality Management System (QMS) based on the ISO 9001 standard. ServiceNow has a dedicated QMS team, quality engineering team, and compliance team to ensure continual improvement.

A note about GDPR

The General Data Protection Regulation (GDPR) is not listed as a certification held by ServiceNow because GDPR is not a standard — it is a regulation (i.e., a law). ServiceNow complies with applicable laws in all jurisdictions in which it operates.

Find out more about the ServiceNow response to GDPR here.
Physical and logical architecture

Overview of physical architecture

The physical architecture supporting the ServiceNow private cloud is deployed into dedicated, ServiceNow-managed colocation spaces, implemented globally. In these locations, dedicated ServiceNow onsite personnel exclusively provide management, installation, maintenance, and support.

ServiceNow builds and deploys Pre-Integrated Racks (PIRs) for all server and appliance infrastructure and cabling, and rack design standards are rigorously enforced. Within each space, multiple levels of redundancy are established for networking infrastructure, internal links, and related components. At a minimum, this network infrastructure is mirrored, both within a single colocation space, and between ServiceNow data center pairs.

Multiple diverse internet connections terminate within these spaces, providing redundant internet access. Servers, appliances, and network devices are multi-homed with redundant components and commodity supplies (i.e., power and network) fed from multiple separate circuits.

Infrastructure operations management

As a Cloud Service Provider (CSP) ServiceNow is responsible for providing and managing the underlying infrastructure on which instances of the Now Platform are deployed. A number of complementary activities and processes are undertaken in managing this environment, all using ServiceNow products.

- **Capacity management**
  A capacity management team ensures the private cloud is able to support current and anticipated future load.

- **Configuration management**
  Continuous monitoring is undertaken to validate the configurations for each of the system and application components that makeup the private cloud.

- **Change management**
  ServiceNow adheres to a rigorous change management process that includes mandatory online training for all ServiceNow personnel with an operational role. Change management processes adhere to ITIL v3 principles. ServiceNow processes thousands of changes each month.

Global data center pairs

The ServiceNow data centers are arranged in high-availability regional pairs, spanning five continents: Asia, Australia, Europe, North America, and South America.
All customer production data is stored in both data centers within the pair and kept in sync using real-time database replication. Both data centers are active at all times, each with the ability to support the combined production load of the pair.

ServiceNow maintains continuous, asynchronous replication from the database in the current primary data center (read-write) to the secondary data center (read-only).

ServiceNow uses top-tier global data center providers. These providers have no logical access to any ServiceNow systems, or customer data, and solely provide private colocation spaces and environmental resources.

Only ServiceNow personnel with a direct responsibility for (or role in) maintaining colocation spaces are able to physically access data center locations.

Meeting regulatory and sovereignty obligations is a significant factor in ServiceNow selecting data center facilities within specific geographic boundaries.

**Data sovereignty**

Data is subject to the laws of the country in which the data is physically stored and to the jurisdiction to which the data subject belongs (e.g., in the case of GDPR).

ServiceNow ensures that data is hosted in data center pairs, where both members are either within the same jurisdiction or within mutually compatible jurisdictions — this means that even when data is transferred from one data center to another, the sovereignty of the data is preserved.

**Storing vs. hosting**

The storing and hosting of data are two distinct concepts, and ServiceNow only hosts customer data. Metaphorically, ServiceNow provides a box and secures it (hosting) and customers decide what they put into that box (storing) as well as who can access that box.

**Data center physical security and environmental controls**

Data centers procured by ServiceNow are provided by specialist colocation data center operators. These operators provide ServiceNow with a secure and reliable space to operate in. The data centers are highly secure facilities with 24/7 security guards, CCTV, multiple levels of entry controls, and strict procedures for physically entering the facility.

Data centers feature a hardened exterior perimeter with defense-in-depth provided by various access control boundaries. Within each data center, all ServiceNow equipment is stored in one or more dedicated, anonymous, cage spaces or private suites.

The details of individual data centers may vary slightly; however, all facilities have similar operating characteristics. In all cases, contractually, the data center providers must be either ISO/IEC 27001 accredited and/or conduct regular SSAE18 SOC 2 Type 2 audits.
Data center physical boundaries

All data centers have external anti-climb fencing, crash resistant walls, and data center halls that are not directly adjacent to exterior walls. Some locations also feature anti-vehicle bollards.

Data centers are divided into zones: public, internal, power, environmental, UPS and battery rooms, loading bays, and others. Although the details of the zones will vary between the data centers, the principle applies across them all. Access controls are applied to each zone in the data center to prevent the movement of unauthorized staff between zones.

The external perimeter of all data centers is lit to allow CCTV systems to provide detailed views of entrance and exit points. Some data center locations also include motion detection systems on the exterior.

Within the data center’s physical boundaries, ServiceNow has its own dedicated cages, or suites, enabling isolation from other data center tenants, including biometric secondary access controls.

Physical intrusion detection

All data centers that ServiceNow operates from have extensive recording CCTV systems internally, as well as at the perimeter. Low light cameras and lighting are used to ensure that details such as facial features and number plates can be clearly identified, even at night.

Typically, recordings are held for at least 30 days, although the length of recording varies from data center to data center. Only authorized personnel have access to the recording systems (controlled by ACL), and all access is audited.

Entrances and exits are alarmed both externally for opening and internally for being jammed open. Exterior glass is alarmed for breakage, and data center floors are windowless.

Data center providers are contractually obliged to notify ServiceNow in the case of security incidents. Activities surrounding this obligation are assessed by audit.

Security guards

Appropriately cleared security guards are present at each data center. The security guards manage the exterior gates and reception areas/front desk, respond to alarms, and conduct scheduled and random patrols of the facilities. All security guards are trained in the operational procedures of the data center.

Facility access control

The data center operators control access to their facilities via multiple levels of locking mechanisms. While the precise details of the individual data centers vary, all data centers make use of a mixture of access control mechanisms, including mechanical, biometric readers, and access card readers requiring PIN entry.

Interlocking mantraps are used to control movement between reception areas and corridors that lead to data center floors. Data center access logs are retained for audit purposes. The retention period of these logs varies across providers.

Data center access control systems prevent staff from entering any area where they are not permitted. ServiceNow maintains access control lists for its own cages and suites, only permitting limited access for data center personnel where absolutely necessary (i.e., for health and safety purposes).
Physical access audits
ServiceNow maintains, and regularly reviews, visitor access logs for its cages or suites. Both physical and electronic records of access are made, and ServiceNow requires its data center providers to supply these logs on a regular basis.

Electrical systems
ServiceNow data center providers typically offer a minimum of 99.982% uptime or the TIA942 Tier 3 standard. These levels of reliability are achieved through the use of redundant power providers, where available, multiple redundant power distribution paths, generators, UPS systems, multiday fuel suppliers, and multiple independent fuel suppliers. As data center pairs are generally geographically diverse, each data center receives power from a different supplier, wherever possible.

Generators and transformers in the data centers are at least N+1 enabled, with distribution networks being either N+1 or 2N. Within the data center, ServiceNow will power devices from disparate distribution networks to ensure that loss of electricity supply on one power networks does not affect others. Uninterruptible Power Supply (UPS) is provided either by battery or flywheel systems that can sustain systems until generators can be activated.

Data centers can typically operate for at least 24 hours at full electrical load without the requirement of additional fuel.

Environmental controls
The Heating, Ventilation, and Air Conditioning (HVAC) systems in the data centers maintain the humidity and temperature within the data center at an optimal level.

Data centers are N+1 redundant for all environmental controls. If humidity or temperature within a part of the data center breaches the parameters defined for that zone, alarms will be triggered, notifying building management to resolve the issue.

Fire detection and suppression
All data centers feature fire detection and suppression systems. The specific system implemented may vary among data centers.

Fire detection is provided by Very Early Smoke Detection Apparatus (VESDA) and heat alarms that are monitored on a 24/7 basis. Fire suppression may be multi-zone, dry-type, double interlock pre-action, and zoned gaseous-based systems, or a combination of both. Fire extinguishers are located throughout the facilities, and exit signs are prominently displayed.

Logical access to ServiceNow infrastructure
ServiceNow employees may be required to access the ServiceNow cloud infrastructure for administration and management of servers, databases, and other components used to provide the service.

In accordance with the separation-of-duties best practice, ServiceNow personnel with physical access to data centers do not have logical access to data environments, and staff with logical access to data do not have physical access to data centers. Similar segregation of duties applies between ServiceNow personnel responsible for managing the key management appliances and the personnel responsible for managing the infrastructure.

The private cloud environment is both physically and logically isolated from the ServiceNow corporate environment and is also subject to different standards, policies, and governance reflecting its different purposes and dispositions.

Critical resources and files are protected by mandatory access controls available in SE Linux Preventive Mode. File Integrity Monitoring is also enabled for critical and sensitive files.

All infrastructure changes are required to go through a series of change management procedures, including approval from the Change Advisory Board (CAB).

ServiceNow does not outsource any service, operational, or management functions that would give a third party access to systems hosting customer data or to customer data itself.
Overview of logical architecture

Today it is more important than ever to understand the fundamental differences between multi-instance and multi-tenant infrastructures. The ServiceNow logical architecture uses a multi-instance single-tenant infrastructure.

Multi-tenant infrastructure — provides limited visibility and control over customer data. In this environment users share the database, so if the database goes offline, every user is affected. In addition, scheduled maintenance must be completed in predefined windows of time, which can compromise availability and security.

Multi-instance infrastructure — provisions a dedicated database for each customer instance, ensuring that there is no possibility of accidental co-mingling of data. This environment offers on-premise-level cloud security with the same, or better, security controls. With multi-instance architecture routine maintenance, including upgrades and issue resolution, occurs individually, making the process quick and easy. Since each instance has a unique database, visibility and control occur natively.

Key benefits of the highly defined and dedicated ServiceNow environment:

**Automation**
Many activities in the ServiceNow infrastructure are conducted entirely using automation, with minimal to zero human interaction. For example, where ServiceNow provisions new instances for its customers, this is a completely automated process. Using this approach as an operational pattern creates consistent configurations, expected outcomes, and reduces the potential for, and impact of, human error.

**Support, scalability, security**
ServiceNow is solely focused on supporting one service: the Now Platform. This is deployed in a private cloud environment dedicated solely to this purpose, and implemented identically in all regions in which ServiceNow operates. The cloud environment supports thousands of identically provisioned Now Platform instances allowing for significant economies of scale and operational agility. The security risks in a highly homogenous service are often more predictable and easier to manage than in highly diverse environments, typical of many enterprises. ServiceNow is focused on only one thing, securing data processed within its infrastructure on instances of the Now Platform.

**Control**
ServiceNow fully manages the underlying software, services, and supporting infrastructure as well as the software development lifecycle. This allows ServiceNow complete control over all components in its environment and vastly reduces supply chain risks.

**SSH (Secure Shell) access**
Access to the Now Platform infrastructure is only permitted through controlled and encrypted SSH sessions initiated over a VPN (with MFA required).

ServiceNow operational personnel must use a secure virtual desktop environment, accessible only from ServiceNow issued endpoints identified by digital certificates. Access requires two-factor authentication and takes place within a virtual environment. Employees cannot extract or copy data from that virtual environment.

The SSH sessions are decrypted for auditing so that all session activity can be fully monitored and recorded. Infrastructure log data is forwarded to a central Security Incident and Event Monitoring (SIEM) solution for analysis, reporting, and alerting. Host-based data leak prevention (DLP) is also enabled.

All SSH access is controlled using a proxy and a centralized Privileged Access Management (PAM) solution is used to manage authorization and monitoring of any commands that require elevated privileges. Only the minimum required privileges are granted for a specific task. ServiceNow manages the privileged entitlements to the infrastructure by job roles and performs a review of privileged access quarterly, to ensure correct entitlements are in place.

**Infrastructure key management**
Encryption keys used in the ServiceNow cloud infrastructure are managed by ServiceNow.

Keys are stored in redundant Key Management System (KMS) appliances.

Key management is performed by a specific dedicated team within the security group, including management of the appliances used to store the per customer instance wrapper key.

Standard operating procedures are used for the procurement, generation, and configuration of key appliances.
**Internet services layer (proxy layer)**

Customers and web services connect to the ServiceNow private cloud over HTTPS using Transport Layer Security (TLS), TLS 1.2 as a minimum, for communication to and from a Now Platform instance.

All interactive end-user activities are performed using a standard web browser. There is no requirement for customers to install any client software on any desktop, laptop, tablet, or smart phone in order to access their Now Platform instances. However, for additional convenience, ServiceNow offers native mobile apps for iOS and Android.

The proxy layer forwards requests from customers’ end-users, or integrations, to the relevant customer instance. This first tier of the application architecture includes network routers, switches, load balancers, firewalls, and intrusion detection systems. All are deployed at a minimum 2N basis (a fully redundant mirrored system with two independent distribution systems). Translation of Universal Resource Identifiers (URIs) to ServiceNow internal IP addresses is also performed in this tier.

**Application layer**

Application servers in a discrete network segment are in the second tier. These servers are accessed only via the proxy layer and are not directly accessible from the internet. They host clustered application nodes for each customer’s instance.

Now Platform instances are the termination point for all inbound requests made by end users to that instance. Requests are received and processed by application nodes (including being escaped or encoded as required) before passing to the relevant database service in the database server tier.

Application and database servers have protections, such as host-based and network-level default deny firewall rules, in place to prevent host-level traffic from reaching the Internet.

**Database layer**

The third and final tier consists of database servers, again installed in a discrete, non-internet routable network segment. Requests from end users, or integrations, cannot be made directly to the database tier and are only issued from a customer’s Now Platform instance.

Each instance has a single database on a database server running multiple discrete and segregated database services. There is no commingling of any customer data between instances and databases: If a customer has four instances of ServiceNow, they will have four entirely separate databases and database services, one unique to each instance.

A significant benefit of the ServiceNow architecture is that it creates a very distinct logical boundary between the data of each customer. This boundary is not dependent on data separation approaches commonly used by many SaaS providers, such as tagging data in shared databases in order to identify which customer it belongs to.

The unique multi-instance ServiceNow architecture enables a highly accurate inventory of the exact location of a specific customer’s data at any given time. Customers can access this information directly via the ServiceNow customer support portal at all times.

The multi-instance tenancy model also enables:

- The smooth transfer of customer instances from one application server to another, within a single data center
- Rapid failover of instances from one data center to another, within the same region
- The ability to perform upgrades and maintenance on an individual basis without impacting other customers’ instances, enabling exceptional instance availability
**Availability**

**Advanced High Availability (AHA) overview**

The ServiceNow data centers and cloud-based infrastructure are designed to be highly available, with redundant components and multiple network paths to avoid single points of failure. At the heart of this architecture, each customer application instance is supported by a multi-homed network configuration, with multiple connections to the internet from different providers and with redundant power sources.

ServiceNow data centers are arranged in pairs, with all customer production data hosted in both data centers simultaneously. These pairs are kept in sync using asynchronous database replication. Both data centers are always active in a main-main relationship with data replicated from the active (read-write) data center to the passive (read-only) data center. Each single data center in a pair is implemented so it can support the combined production load of both locations.

Within each regional data center pair, there is no concept of a fixed primary location for any customer instance. For example, a customer with two separate instances could have them operating out of different data centers simultaneously.

![Diagram of AHA Transfer](image)

ServiceNow leverages AHA for customer production instances for the following purposes:

- Prior to executing maintenance, ServiceNow can proactively transfer operation of a customer instance from one data center to the other. The maintenance can then proceed without impacting service availability.
- In the event of failure of one or more infrastructure components, service is restored by transferring the operation of the affected instance to the other data center.

With this approach, the transfer between active and standby data centers is regularly executed as a standard operating procedure. This ensures that when it is needed to address a failure, the transfer will be successful, minimizing service disruption.
Transfer and failover

ServiceNow has two distinct processes related to ensuring instance availability: transfer and failover.

Transfer

A transfer of an instance is a scheduled event, usually performed for maintenance purposes. These outages occur within the contracted availability service level agreement that ServiceNow commits to with each customer.

Failover

A failover of an instance is an event usually performed when availability for one or more customer instances cannot be maintained. This could be caused by a local component failure, or an event such as a major environmental incident or resource outage.

In the case of a local component failure, a failover to a system within the same data center will be attempted first. If a data center-wide outage is identified, all current active production instances in the impacted data center will be failed over to the passive data center location in the pair. In this circumstance, a Recovery Time Objective (RTO) of two hours, and a Recovery Point Objective (RPO) of one hour is targeted. Due to the almost real-time replication between data center pairs, these times are often significantly shorter than the stated RTO/RPO.

Automation technology built on the Now Platform is used to transfer or failover instances, when necessary. The mechanism for both processes is very similar. The current passive system is designated active, and vice versa. To complete the process, DNS mappings and instance database configurations are updated accordingly. Redundant DNS providers and DNSSEC (Domain Name System Security Extensions) are employed to provide robust, resilient name resolution services.
**Data backup and recovery**

The ServiceNow Advanced High Availability (AHA) architecture is the primary means to restore service in the case of a disruption that could impact availability. However, in certain scenarios, it may be desirable to use more traditional data backup and recovery mechanisms. For example, such circumstances could include a customer deleting data inadvertently, or a customer's data integration or automation is misconfigured or malfunctions — resulting in data being rendered unusable or inaccessible. In these scenarios, the high availability technology could not assist. Restoring from backup would be the only option for recovery.

Full backups are performed direct to disk every seven days, with differential backups performed every 24 hours. These backups are retained in accordance with ServiceNow standard operating procedures, after which no record of deleted data will remain in the ServiceNow infrastructure. Backups are stored in the same data centers where the data resides, with production instances backed up in both data centers in the pair. Sub-production instances (commonly used for testing and development purposes) are backed up only in their primary data center, as they are not AHA capable.

All backups are written to disk. Tapes and removable media are not used. Backups are not sent off-site, but they are performed on both data centers in a pair, therefore benefiting from geographic separation. At the end of their working life, the disks used for the backups are securely wiped and/or destroyed, to comply with data sanitization requirements.

Backups are encrypted with AES-256 using randomly generated encryption keys for every backup. These keys are kept in a secure key store and are only retrieved by an automated process, if a data restore is initiated. Regular, automated tests are run to ensure the quality of backups, and any failures are reported for remediation within ServiceNow.

The ServiceNow backup architecture is not designed to provide archival records, in accordance with the ServiceNow Standard Operating Procedures (SOPs). However, customers may retain data within their instances for as long as they require, in accordance with their policy or regulatory requirements. Additionally, there are capabilities available within the Now Platform to allow customers to manage logs and regularly export data to external systems, if needed.

**Business continuity and disaster recovery**

ServiceNow is divided into two distinct environments for the purposes of Business Continuity (BC) and Disaster Recovery (DR). The ServiceNow corporate IT environment and its cloud data centers are both physically and logically isolated from each other. A disaster affecting the ServiceNow corporate environment could occur with little or no impact on the ability of the private cloud data centers to continue to operate.

In both cases, the BC and the DR procedures are supported by a series of tested processes, automations, and supporting documentation, allowing ServiceNow to quickly and effectively take action when availability of its cloud, or critical supporting services, are affected.

**Execution**

The ServiceNow Information System Contingency Plan (ISCP) covers its cloud data center environments. The ISCP scope includes all customer instances of the Now Platform, as well as those ServiceNow uses internally (as an organization) to support its business. The ISCP uses the ServiceNow Advanced High Availability (AHA) architecture.

**Testing and compliance**

ServiceNow formally tests its recovery processes on an annual basis and can produce reports relating to this for customer review. ServiceNow also uses the process of transferring instances, for maintenance purposes, on a daily basis. As a result, ServiceNow is very well practiced at the process of “failing over” or transferring customer instances.

**Organizational business continuity**

The ServiceNow organizational business continuity process covers its corporate environment and functional offices. It is therefore a separate process from that used in its cloud environment. The Business Continuity Plan (BCP) has been developed in collaboration with the entire business and includes ongoing Business Impact Assessments (BIA) to understand the impact of the loss of any given systems, services, or physical locations.

Read more about the ServiceNow highly available cloud infrastructure in the [Advanced High Availability (AHA) architecture](#) white paper.
Software Development Lifecycle (SDLC)

Secure software development

ServiceNow uses an agile development process that includes independent validation steps run by a separate quality team. A requirement of this process is to produce a validation report that includes security as a required signatory to the release process. This allows effective prioritization of remediation efforts and provides security feature requests to the application.

Developers and other relevant personnel are trained on an ongoing basis through a variety of methods, including classroom-based training that covers web application security.

Application security teams

The ServiceNow Security Office (SSO) has dedicated teams of security engineers who are deeply integrated into the overall software development program. The teams perform a number of functions, including but not limited to:

- Managing the various internal and external testing programs
- Performing assessments of internal ServiceNow services and organization instances used for running its business
- Performing architectural reviews of new features and security features
- Curating educational security materials, including those for customers

Application security testing

The ServiceNow penetration testing program is a vital component of its development practices and is therefore wide-ranging and extensive.

Testing during development

During development, code for the Now Platform is subject to continuous ongoing testing, and review, using a variety of methods within ServiceNow. Third-party commercial and in-house automated toolsets are used for static and dynamic application security testing. Additionally, manual testing and code peer reviews are also conducted. These efforts are all focused on security and detection of vulnerabilities at the application code level.

Any validated security issue found is also checked for and, if necessary, remediated in supported versions of the Now Platform. This remediation is provided either in the next patch for that release or as a hotfix, subject to criticality.

Application penetration testing

After internal testing, external application penetration testing is carried out, providing independent review and transparency around the ServiceNow secure development practices. A third-party organization is given access to the resources necessary to review and test the next release of the Now Platform for an extended period of time, before it is made available to customers.

After completing a first round of testing, any confirmed issues are entered into the ServiceNow problem resolution process, prioritized, and categorized. Issues that meet predefined ServiceNow criteria for impact and criticality are remediated prior to any re-testing.
Once the remediation is complete, the same third-party organization conducts a second round of testing to confirm the provided remediation or mitigation functions as expected.

Results of the third-party testing are consolidated into an executive summary report accessible to customers from the ServiceNow CORE Compliance Portal. Find out how to access CORE here.

**Customer application penetration testing**

Another significant aspect of the ServiceNow application penetration testing program involves tests performed by its customers on their own Now Platform instances. Customers are permitted to perform one penetration test per calendar year.

Testing scheduling must be pre-approved and conducted at a date and time agreed upon by ServiceNow and the customer. This is necessary for ServiceNow to continue conducting its monitoring activities and to differentiate potential attacks from authorized customer testing.

As a condition of testing, customers are required to share the validated steps to reproduce any finding with ServiceNow, in accordance with the documented process.

Validated customer findings help contribute to the collective security of the ServiceNow environment and enable a continuously improving security posture. The customer penetration testing program supports a significant number of tests annually, across the customer base.

Once validated by ServiceNow, confirmed vulnerabilities discovered by this process are remediated according to the ServiceNow vulnerability management criteria.

Release notes for each major version, patch, and hotfix on the ServiceNow docs site contain information regarding what has been remediated in each release, including remediations that are security-related.
### SDLC prevention mechanism table

This table summarizes some of the major mechanisms in place at ServiceNow to prevent or mitigate addition of malicious code to the codebase during the ServiceNow SDLC process. This table is not intended to be an exhaustive list.

Code additions made by third-parties are heavily scrutinized and reviewed. Throughout the ServiceNow SDLC process, new internal code is controlled via a group, along with a sequence of checks, validations, and approvals.

<table>
<thead>
<tr>
<th>Prevention Mechanism</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controls on who can access ServiceNow source control system</td>
<td>The ability to add code to the ServiceNow codebase is limited to specific roles. Access must be requested and granted by a manager, as detailed in the <a href="#">Code Control SOP</a>.</td>
</tr>
<tr>
<td>Read-only access to code, where possible</td>
<td>Applying the principle of least privilege, functions that require only read access to codebase (a support role, for example) get a special role that prevents them from pushing code or writing to the codebase.</td>
</tr>
<tr>
<td>Control over third-party additions or dependencies</td>
<td>Any new import or addition of a third-party package is flagged and requires Engineering and Legal approval in order for the import to be merged to the main release branch.</td>
</tr>
<tr>
<td>Team branches</td>
<td>Developers are not allowed to push code directly to the main branch of the codebase. Instead, dedicated branches are created for teams, and team branches get merged (up to the main branch) through a series of checks and processes.</td>
</tr>
<tr>
<td>Code reviews</td>
<td>Code reviews occur within each team branch. Commits specific to the branch must be approved by another member of the team before being pushed. Git logs and history of commits are also reviewed as part of the merges up the main release branch.</td>
</tr>
<tr>
<td>Strong association of code commits to SDLC artifacts</td>
<td>Any git commit must be associated (by specifying an identifier in commit message) with a story or defect for traceability. Commits that do not follow this rule get high scrutiny.</td>
</tr>
<tr>
<td>Merge verification process</td>
<td>As part of merging team branches to the main branch, a number of automated scans and checks are performed. These include changes such as addition of new metadata tables/types, code check-ins without artifacts, artifacts without code check-ins, localization issues, and test failures. Impactful changes must be tied to an approved Architecture Review Board ticket.</td>
</tr>
<tr>
<td>Daily metrics and checks</td>
<td>Each branch gets test runs and daily metrics measuring changes to a set of predefined common flows on the product. Any delta in transaction processing, sql time, sql count etc., are flagged and prevent a merge to the main branch, until justified and approved.</td>
</tr>
<tr>
<td>Security scans and firewall</td>
<td>Frequent scans are applied to the codebase to flag suspicious, harmful, or insecure code: credentials, cryptographic usages, known vulnerabilities etc. Those flags also require review and approval. The final build undergoes a third-party penetration test prior to being released for general availability.</td>
</tr>
</tbody>
</table>

For more details on the ServiceNow SDLC processes see the [Code Control SOP](#) (requires access to the ServiceNow Core Compliance Portal, find out how to access [here](#)).
Information lifecycle and data management

Information classification
ServiceNow applies relevant data classification levels to all customer data it hosts. ServiceNow does not inspect or monitor its customers’ data and has no ability to understand how any data may have been classified by individual customers. For ServiceNow, the overriding requirement towards customer data is that it remains hosted solely in the private cloud and is treated and handled according to its policies for all customer data.

Customers remain the data controller (i.e., data owner) for all data they store in their Now Platform instance and should therefore apply controls according to their data classification policies.

Data retention
As the data controller, customers decide what information is to be stored, how it is to be used, and how long it is retained. ServiceNow does not delete or modify customer data and only processes data in accordance with its contractual obligations.

Backups are retained in accordance with ServiceNow standard operating procedures, after which no record of deleted data will remain in ServiceNow infrastructure. At the end of their working life, disks are securely wiped, or destroyed, such that no data remains.

Media disposal
ServiceNow hosts its customer data on Solid-State Drives (SSD) or mechanical disks across and within its data center colocation spaces. Tapes and other forms of removable media are not used in providing the service, including for backups (which are also written to disk).

Functioning mechanical storage devices that are retired at end-of-life, or for re-assignment to new customers, are logically shredded based on NIST (National Institute of Standards and Technology) best practices. SSD drives are securely erased with processes utilizing appropriate tools provided by the relevant SSD hardware vendor.

All failed storage devices, both mechanical and solid state, are securely retained within the same data center colocation space where they resided, regardless of whether they contained customer data or not.

Data return and destruction
Throughout the lifetime of the subscription, data can be directly exported using features available in a Now Platform instance. This can be via the user interface, through integrations, or by using optional ServiceNow components such as the available Open Database Connectivity (ODBC) connector or MID Server.

At all times during the term of the contract and prior to termination or expiration of the agreement with ServiceNow, customers can self-export their data from their instance using features in the Now Platform. Customers can also request that ServiceNow export their data in a standard format. Please see Exporting Data from the product documentation for more details.
ServiceNow security operations management

Infrastructure vulnerability management
ServiceNow maintains an ongoing infrastructure vulnerability program using third-party commercial and in-house tools to identify vulnerabilities in the ServiceNow perimeter and for all cloud and corporate systems.

Identified vulnerabilities feed into the overarching vulnerability monitoring and remediation program. As necessary, patching of affected systems, services, or applications is undertaken promptly, in accordance with ServiceNow criteria and processes.

Infrastructure vulnerability scans occur monthly for public facing infrastructure on an unauthenticated basis. Monthly scans are also performed on an authenticated basis for internal, non-internet routable infrastructure.

Operating system security
ServiceNow builds and maintains standard network device, appliance, and operating system build configurations. New devices and servers are deployed with automatic configurations relating to their function and these are reapplied on an ongoing basis when changes are detected.

Controls relating to the monitoring of sensitive operating system files and restrictions on lateral movement across data centers are also in place. Anti-malware measures, with regular updates, are made to all servers within the private cloud, as well as all ServiceNow corporate IT systems and endpoints.

Infrastructure and application security services
ServiceNow has intrusion detection capabilities within its private cloud. All relevant services and system components send security logs and events to a Security Information and Event Management (SIEM) for security monitoring and alerting. See Logging and monitoring: ServiceNow security infrastructure for more details.

Distributed denial of service (DDoS)
ServiceNow employs a significant range of detective controls to monitor and prevent potential distributed denial-of-service (DDoS) attacks from impacting the ServiceNow private cloud environment. These controls include the implementation of in-house DDoS protection mechanisms, provision of significant Internet bandwidth connectivity, and the use of third-party protective services to mitigate against such attacks.
Vulnerability management

Now Platform vulnerability management

ServiceNow produces two releases of the Now Platform annually. In addition, patches and hotfixes are produced throughout the supported lifetime of a major release and rolled into the codebase for inclusion in the next version.

To ensure customers are benefiting from the most current security, performance, and functional fixes, ServiceNow will apply patches to customer instances on a continual basis as part of the ServiceNow Patching Program. Each quarter, one full patch and two security patches will be automatically scheduled to update a customer’s instance(s).

An instance of the Now Platform may continue to be used while a major release upgrade, patch, or hotfix installation takes place. Patch application leverages the Advanced High Availability capability and results in minimal impact to service when any update is applied.

ServiceNow requires customers to remain on a supported release of the Now Platform and will actively engage with customers’ risk and security personnel to highlight the risks of non-compliance.

Cloud infrastructure vulnerability management

Findings reported from the continuous scanning of its infrastructure by the ServiceNow vulnerability management tools are automatically logged within an internal Now Platform instance. These findings are first reviewed by ServiceNow personnel to determine that the appropriate level of priority is assigned, taking into account such factors as relevant mitigating controls and exposure. Issues identified at the highest risk classification level will be targeted for remediation as quickly as possible.

The ServiceNow infrastructure stack is customized at each layer to support the Now Platform specifically. Publicly identified vulnerabilities in common software platforms, e.g., CVEs (Common Vulnerabilities and Exposures), may not necessarily present a risk within the context of the Now Platform. This can be due to factors such as the absence of the affected software or component in the ServiceNow environment or its limited or complete inability to access the Internet.

Once ServiceNow determines that a patch needs to be deployed, this effort enters the change management process. During this process, the assets, risk, and potential impact to the relevant environment are identified along with the testing required, back-out plan, and timeline for deployment. When no clear remediation is available, virtual patching is implemented.

When performing infrastructure maintenance such as patching, ServiceNow leverages the Advanced High Availability architecture to transfer a customer’s production instance between data centers, thereby minimizing the impact to availability.

ServiceNow does not condone any attempts to actively audit our infrastructure. However, ServiceNow recognizes that vulnerabilities in our systems, products, or network infrastructure are occasionally discovered incidentally. If vulnerabilities are discovered, they should be reported to ServiceNow in a responsible manner per the Responsible Disclosure Program.

Instance integrations

Overview of instance integrations

The Now Platform is based on Service-Oriented Architecture (SOA). To support customer workflows, all data objects can use web services to access bidirectional data-level integrations. Integrations may be implemented programatically or through the use of features in the Now Platform, including IntegrationHub, to simplify and accelerate customer integrations.

The Now Platform also offers a rich interface for loading external data, using import sets which allow customers to load from different data sources such as HTTPS, FTPS, and SCP using file formats such as XML, CSV, and Microsoft Excel files. Information can also be pulled from a data source using a direct JDBC (Java Database Connectivity) connection, provided customer network connectivity permits it.

For integration with systems, services, or applications within a customer’s network, the Now Platform provides the MID Server component. This capability enables secure integration and collaboration between a customer’s own applications and services and a customer’s Now Platform instance(s). MID Servers may also be combined with import sets for data sources not accessible to a customer’s Now Platform instance.

Information within an instance can be exported and migrated to an external platform using an Open Database Connectivity (ODBC) driver provided by ServiceNow. Forms, lists, and reports on the platform can be accessed directly using a URL, which facilitates integration between two or more web applications.
Now Platform MID Server

The ServiceNow Management, Instrumentation, and Discovery (MID) Server is a free, optional, Now Platform component. The MID Server enables data communication between a customer instance and external applications, data sources, and services.

Customers use MID Servers in conjunction with their instances for enterprise application and service monitoring, integration, orchestration, and discovery.

The MID Server is a Java application, provided to customers via a download link within their instance. This application can be installed by the customer admin on a suitable host system within their environment and is compatible with Windows or Linux operating systems.

MID Servers are cryptographically paired with an individual instance during installation and must be approved by the Now Platform customer administrator before the MID Server can be used.

At a customer-defined interval, a MID Server securely initiates an outbound session to a customer’s instance over HTTPS using TLS (TLS 1.2 as a minimum), looking for activities to perform. Once activities are identified they are retrieved and executed and any output, or resulting data, is returned to the originating instance.

This outbound, or “pull” approach negates the need to permit inbound access through a customer’s perimeter, or firewalls, directly to the Internet.

MID Server diagram

Web services integration

The Now Platform supports web services using SOAP (Simple Object Access Protocol) and REST (Representational State Transfer) for integration, all traffic is encrypted using TLS (TLS 1.2 as a minimum).

Web service security is enforced using a combination of basic authentication challenge/response and system-level access using contextual security. Additionally, the web service user may be granted a set of web service-specific roles.

For incoming SOAP requests, support for WS-Security 1.1 in the form of WSS X.509 token profile and WSS username token profile is available. In this context, “incoming” means requests targeting a web services resource in a customer Now Platform instance.

Mutual web services authentication is supported for inbound and outbound HTTPS connections, such as SOAP, REST, or direct HTTPS calls, as well as those sent through a MID Server. Global API policies and secure signing of SOAP requests for message integrity purposes are also available.
Now Platform malware protection

Now Platform instances feature antivirus software that protects against uploading or downloading malicious content. File attachments are scanned by dedicated servers, in each regional data center, to guard against viruses or malware being distributed from an instance.

Instance communication hierarchy

Customers initiate communication from their network to their Now Platform instances over HTTPS from any endpoint device with a browser, or from a system or application level integration.

An instance never initiates communication into the customer’s network unless a data source or other integration within the customers environment is configured by the customer themselves.

Activities such as ServiceNow Discovery or Orchestration that can “touch” customer infrastructure are executed only at the customer’s direction. These are via activities that the customer admin defines in their instances and actioned using MID Servers they have deployed. Output that is produced as part of an activity is sent back to the relevant instance over HTTPS.

Customers can place as many MID Servers in their environment as required to support any network topology, ranging from a flat, to a highly segmented network.

Accessing data

As the data controller, the customer determines who has access rights to their instance and the data stored in it.

As the data processor, ServiceNow provides the tools for customers to secure and audit their instance according to their requirements.

Authentication

A Now Platform instance provides a customer with a number of authentication options that can be used simultaneously, using a multiple authentication model:

- **Multi-Provider Single Sign-on (SSO)**: External SSO allows organizations to use several SSO Identity Providers (IdPs) to manage authentication as well as retain local database (basic) authentication.
- **LDAP**: An LDAP integration allows a customer’s instance to use their existing LDAP server as the primary source of user data.
- **OAuth 2.0**: Allows users to access instance resources through external clients by obtaining a token, rather than entering login credentials with each resource request.
- **Digest Token Authentication**: The digest token authentication passes user credentials and a digest token within an unencrypted HTTP header. The instance reads the HTTP header value and compares its computed hash value of the digest token. If the computed hash value matches the digest token value, then the instance searches for a matching value in the user table. If there is a matching value in the user table, the instance considers the user pre-authenticated and logs the user in. The hash operation is user-specific such as SHA1, SHA 256, or MD5. The hash value has to be appended as part of the URL suffix, which works on the query parameters.
- **Time Limited Authentication**: Admins can configure link-based time limited authentication on a Now Platform instance. The configured link can be shared with the user through Email or SMS, then the user can use that link to login to the instance.
- **Multi-factor Authentication (MFA)**: Passcode from QR code, which includes a secret code at bottom with the information such as instance name, username or user account information, and code for authentication.
- **Certificate-based authentication**: mutually authenticate user logins or inbound API requests using certificates from a trusted Certificate Authority (CA).
- **Local database**: Username and password authentication of a customer’s user record, stored in the instance database.
- **System for Cross-domain Identity Management (SCIM)**: The System for Cross-domain Identity Management (SCIM) API provides endpoints to create, read, update, and delete operations on users and groups using the SCIM protocol.
The **Adaptive authentication** policy framework can be used to enforce contextual authentication controls to the right users at the right time. Adaptive authentication uses authentication policies to evaluate authentication requests, then either deny or allow access to a customer instance based on the specified policy conditions. Adaptive authentication policies and contexts can be used to restrict access to an instance for users and APIs based on criteria like IP address, user role, and user group. Customer admins can configure the built-in authentication policies according to their security requirements.

**Security Assertion Markup Language (SAML) for Single Sign-On (SSO)**

The Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data between security domains. SAML exchanges security information between an Identity Provider (a producer of assertions, commonly abbreviated to IdP), and a service provider (a consumer of assertions).

The Now Platform SAML 2.0 integration enables SSO by exchanging XML tokens with an external IdP. The identity provider authenticates the user and passes a NameID token to the Now Platform instance. If the instance finds a user with a matching NameID token (e.g., the email address), the instance logs that user in.

Customers can use the Identity Provider attributes that are received from the SAML response from the IdP as a filter criteria for authentication.

The Now Platform SAML plugin supports SSO-based authentication via a variety of SAML-compliant identity providers. This includes Active Directory Federation Services (ADFS), as well as third-party identity providers such as Ping, SecureAuth, SailPoint, Okta, or any providers that are compliant to the SAML 2.0 standard. Customers can use SAML and Digest Authentication through the Multiple Provider SSO application.

Customers who implement their own SAML compliant IdP, or opt for a third-party service, can leverage this with other cloud services. When customers elect to use the SAML plugin, their password and credential policies are governed by their own IdPs.

Multi-factor Authentication (MFA) can be used in conjunction with customer SSO and is highly recommended, especially for privileged users. ServiceNow recommends using built-in MFA for privileged users when employing that option.

Optional Zero-Trust Access allows customers to implement fine-grained access controls based on various factors such as user roles, device health, location, and other contextual information. Zero-Trust enables customers to enforce the principle of least privilege, granting users only the necessary access required to perform their specific tasks.

**Lightweight Directory Access Protocol (LDAP)**

LDAP authentication allows customers use their own LDAP-compliant directory services, such as Active Directory (AD) or similar. Customers who elect to use their own LDAP directories have their password and credential policies governed by the policies set within their directory service. A directory needs to be accessible to the relevant Now Platform instance since these are commonly located behind a firewall, or other perimeter controls. Multiple directory service sources may be configured and secure LDAP (LDAPS) is also supported.

With an LDAP integration, authentication paths begin with end user providing their username and password to the customer’s Now Platform instance. These credentials are then used by that instance to perform a simple bind against the customer’s target directory service for that user. If successful, the user will be authenticated to the relevant Now Platform instance.

As part of the LDAP integration, passwords are neither stored nor transferred back to the customer’s Now Platform instance.

**Built-in “native” authentication**

Another approach to maintaining identity data is for customers to use the Now Platform’s built-in native authentication, especially for privileged users, such as system administrators.

When using native Now Platform authentication, properties such as the length, complexity, rotation, and uniqueness of passwords are customizable by a customer administrator.

**OAuth 2.0**

OAuth 2.0 allows customers to access instance resources through external clients by obtaining a token, rather than by entering login credentials with each resource request.
OAuth 2.0 is implemented in the Now Platform for the following scenarios:

<table>
<thead>
<tr>
<th>Auth external client scenario</th>
<th>Auth provider scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>A customer’s instance provides an endpoint for third-party clients to pull data from the instance.</td>
<td>A customer’s instance pulls data from a third-party provider.</td>
</tr>
</tbody>
</table>

Customers can configure a login experience that is specific to a mobile app and different from the web login experience. For example, Now® Mobile app users can be automatically redirected to an Identity Provider (IdP) that is different from the IdP defined for the web session.

**Authorization**

Customers have full control of entitlements granted to each of their users in a Now Platform instance.

Now Platform instances include built-in Role-Based Access Control (RBAC) mechanisms providing user, group, and role objects. These mechanisms can be used by customer admins to assign access to applications and data, within their instance(s). Customer admins can add additional users, groups, and roles to those already defined.

Access Control Lists (ACLs) are used in conjunction with RBAC to control access to entire tables, records, or fields. A number of default ACLs exist in an out-of-the-box Now Platform instance. Customer admins can add to those, per their own requirements.

ACLs have individual entitlements which include create, read, write, and delete. In addition, access can be further controlled on a contextual basis, depending on individual attributes of the object being accessed. These attributes could include the state of a specific kind of record, the value of a field, or even the day, date, or geographic location of the end user. The attributes available also vary, depending on the type of object being secured.

Because integration with a customer’s own directory services is possible, existing users and groups in those directory services can be used to manage users and access within the customer’s Now Platform instances.

**Customer access management**

ServiceNow customers are responsible for the management of user identities within their instances. This includes the creation of individual identities (credentials) for each of their users, both internal and external, the methods used to authenticate those users, password policies (for built-in authentication), as well as the entitlements, and access levels granted to those users.

**User identity synchronization**

Now Platform instances require every user to exist as an identity within the database, regardless of authentication mechanism. This identity is necessary to support a wide variety of capabilities within the product, including role-based access purposes.

To enable the identity requirement, Now Platform instances support both automated and manual creation of user identities. This includes synchronization of users, their group memberships, and group objects themselves. Customers may incorporate as few, or as many, user attributes as they deem necessary. However, user object passwords cannot be synchronized.

A common approach to maintaining identity data is for customers to use their own LDAP directory. This would be configured in an import set as a data source for user and group objects. Once configured this allows synchronizing the information in a customers’ Now Platform instance with that in their own directory service. Customers can specify the interval, or regularity, of synchronization per their own requirements (which is usually daily, as a recommended minimum).

Customers may also leverage the ServiceNow MID Server component for LDAP synchronization. This component negates the need for customers to allow their Now Platform instances through their perimeter and firewall in order to access their internal directory servers. Instead, customers can install the MID Server inside their internal network, where it can access the directory server and return a payload of users or groups and their attributes to the customers’ instance. These users and groups would then be automatically imported, or updated, in the target user or group tables within the instance.

User and group objects can be uploaded to a Now Platform instance through the use of import sets. These sets can use various types of data sources for user and group objects intended for use with a Now Platform instance. This process is commonly used for initial user uploads, to populate the ServiceNow user and group tables in a customer’s instance. These sets can also be used for ongoing synchronization of user and group tables. Customer admins can also import a flat file that was exported from the chosen authoritative identity source.

If a user exists in a customer’s IdP but is not in the customer’s Now Platform instance, SAML user provisioning can automatically create the user in the instance.
System for Cross-Domain Identity Management (SCIM) is also supported. This allows customers to easily provision and manage user identities, group membership, and other properties from external sources using an industry-standard protocol. These typically include cloud-based services like Active Directory, Amazon Web Services, Okta, and others. Features of the Now Platform SCIM free customers from having to create and manage multiple customized SOAP APIs.

ServiceNow access to customer data
Occasionally, ServiceNow employees may be required to access a customer’s instance to provide support. Access to a customer’s instance is on an incidental, per-event basis, and not every customer support event will require access to customer data.

If a ServiceNow employee incidentally accesses customer data during support activities, it is processed within what is contractually permitted. This data is also protected, to maintain compliance with relevant statutory obligations such as GDPR.

Only members of the ServiceNow support organization who have been specifically assigned to an active support case can be granted access — and that access is granted on a just-in-time basis. Additionally, customers may specify that their explicit authorization is also required when access is requested.

Access can only be gained via a secure virtual desktop environment which is only accessible from ServiceNow data centers that require a client device authenticated by a digital certificate. Users are required to pass two-factor authentication before access is granted. Host-based Data Leak Prevention (DLP) is in place and user activity is monitored, and controlled, with a Privileged Access Management (PAM) system.

Please see "Logical access to ServiceNow infrastructure" on page 16 for more details.

ServiceNow Controlled Access (SNCA)
On occasions when there is a requirement for ServiceNow Support employees to access a customer instance of the Now Platform, they follow strictly controlled procedures. These procedures define which employee roles can be approved for access, how specific authorization is granted on a per-instance and per-employee basis, and how those personnel connect to the customer instance.

Access is temporary and only granted after a support case, or change request, is assigned to an employee. The access is revoked once the activity is closed or reassigned.

Once appropriate approval is obtained, access is provided via the ServiceNow Controlled Access (SNCA) solution. SNCA consists of a regionally deployed, secure virtual desktop environment that can only be accessed after a user authenticates with two-factor authentication from a ServiceNow address space, with a device identified by a digital certificate.

No internet access, email, or messaging is possible from the virtual desktop environment. No data transfer such as file transfers, copy/paste functionality, or device/USB redirection can occur between the virtual environment and host endpoint, or a host-based Data Leak Prevention (DLP) system.

ServiceNow SNC Access Control plugin
Customers can control which ServiceNow employees can access their instance, and when, by using the ServiceNow SNC Access Control plugin.

Once this plugin is activated, access permissions must be explicitly granted to a user, including defining a time frame for access to occur within. Customers can revoke access at any time. All login events are recorded, and if successful, all subsequent activity is logged in detail in the event and transaction logs.

Customers should be aware that the SNC Access Control plugin only restricts ServiceNow personnel’s access to customer instances of the Now Platform. It does not apply similar access restrictions by ServiceNow personnel to the cloud infrastructure on which all Now Platform instances are provisioned.
Security logging and monitoring

Most activities within an instance can be recorded in an audit log, and the Now Platform includes comprehensive access, event, and transaction logging.

The extent of logging is customer configurable, and detailed logging can be used to record and report on all activity within an instance. Logs can be reviewed directly within the Now Platform instance or exported to a customer’s security information and event management (SIEM) tool.

Workflows or incidents can be automatically created based on detected activity. Customers can also enable auditing for database tables, to track and view details of any changes made to data at a record or field level.

In order to detect potentially malicious actions or activities in relation to its service ServiceNow collects and retains logs and events relevant to its entire cloud infrastructure, including information regarding requests made to instances of the Now Platform. ServiceNow uses such log and event management in conjunction with its ongoing operational security and incident management processes. This information is not available to customers within their Now Platform instances. However, events that occur within a specific customer’s instance are accessible to that customer through their instance logs and these events are also captured in the Now Platform infrastructure logs.

<table>
<thead>
<tr>
<th>Log type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction</td>
<td>All browser activity for an instance</td>
</tr>
<tr>
<td>Email and push</td>
<td>All email notifications and push messages sent from all instances within the system</td>
</tr>
<tr>
<td>Event</td>
<td>All system events that occur within the system</td>
</tr>
<tr>
<td>Import</td>
<td>Data import activity within the platform</td>
</tr>
<tr>
<td>Table changes</td>
<td>Changes made to all tables in the system</td>
</tr>
<tr>
<td>Outbound HTTP request</td>
<td>All outbound web services requests, such as REST and SOAP requests</td>
</tr>
<tr>
<td>Signature image</td>
<td>Electronic signatures for the HR signature pad</td>
</tr>
<tr>
<td>System</td>
<td>Warnings and errors for instance processes, records, and non-critical events, such as memory usage on the server machine</td>
</tr>
</tbody>
</table>

Logging and monitoring: Now Platform instances

A Now Platform instance generates detailed log and audit information regarding activities which take place within it. The default application logging capabilities of the Now Platform include verbose transaction, client, event, email, and system logs.

Log information is stored, like all customer data, within tables in a customer’s instance. As with any customer data, ServiceNow does not access this data during normal provision of its service. Customer admins manage and monitor the available logs in their instances, as they would any other information within an instance.

Log and audit data is protected by access control rules in the same manner as all other customer data. Access to log information is usually limited to administrative roles only.

Logs and events can also be forwarded to a customer’s own logging system, or security information and event management (SIEM) environment. This can be achieved using the syslog probe, the MID Server, or by making direct web service calls to the various log tables. Customers may also simply download or export log table entries, or list views, containing items of interest. These techniques allow log and audit events to be stored within a customer’s environment and retained according to the customer’s specific requirements. Options are available for direct customer SIEM integration, which facilitates real-time logging as part of the Now Platform Vault security bundle, or this can be purchased as a standalone option.

Transaction logs represent every click, view, and system event that occurs in an instance. These logs include a level of detail useful for customers when troubleshooting issues, as well as providing detailed intelligence on behaviors within an instance.
Event logs include the creation of an incident, or deletion of a problem, or any one of a number of standard, pre-configured events. Event logs may also be extended to contain customer defined events. Additionally, a number of security-related events are available in the event log. These events include recording successful login, failed login, security privilege escalation, and viewing of tables or records.

In addition to reviewing logs manually, workflows or actions can be executed when a specific event or log entry is detected, or a metric is reached, such as failed logins per minute or access to sensitive administrative roles. These actions could trigger a notification via email, raise an incident to investigate the matter, or even perform an activity against an application, system, or device within a customer’s network.

Audit history is the final aspect of activity logging and recording. This feature records all activities, with respect to data and customizations, within a customer instance. For any particular table or field, audit history may be turned on (or off). The audit history feature then maintains a record of who made any change, when the change took place, and what was changed. A number of tables are audit-enabled by default, and audit history is perpetual for the lifetime of that record.

**Logging and monitoring: ServiceNow security infrastructure**

A key component the ServiceNow security program is to maintain detective controls to monitor for potential threat actors and intrusion attempts into the ServiceNow cloud and corporate environments.

ServiceNow has a formal, documented security incident response policy, process, and workflow. The ServiceNow incident response process includes event discovery, triage, escalation, notification (including customer notification), remediation, and postmortem review.

If a customer’s environment or data is impacted, the customer will be automatically notified. Contractual commitments can be viewed by accessing the [Data Processing Addendum](#) (DPA).

ServiceNow has deployed a redundant Intrusion Detection System (IDS) that monitors network traffic as it transits into its cloud network. Additionally, a host and network-based Data Leak Prevention (DLP) system is used to guard against data transfer and exfiltration from corporate systems, and also between the cloud and corporate networks. These systems feed into the Now Platform Security Information and Event Management (SIEM) systems.

ServiceNow maintains separate SIEM systems for its corporate and cloud environments, with further logical separation for SIEMs tasked with network, device, and security events. Alerts and notifications are generated by the SIEM systems in accordance with predefined triggers and metrics. These alerts are reviewed by a 24/7 security operations team with global coverage.

ServiceNow tunes and adjusts monitoring to meet the specific characteristics of Now Platform instances. For example, approved customer penetration tests need to be differentiated from illegitimate or malicious penetration attempts. The SIEM helps support the processes that enable ServiceNow security operations to undertake such determinations reliably and promptly.

Events, alerts, and relevant logs are also fed into the SIEM from other systems, including all servers, network devices, and ancillary systems. This allows ServiceNow to build and maintain a comprehensive manifest of the activities that are occurring in its environment, on a day-to-day basis. Security alerts, events, multiple threat feeds, and other relevant information are stored and aggregated into an internal Now Platform instance, for ongoing management.

ServiceNow is responsible for managing its SIEM environment and securing the events within it. Separate teams are responsible for the configuration and maintenance of the logging infrastructure and the data it generates, ensuring separation of duties. Network event logs and infrastructure events are retained for a minimum of 90 days.

The ServiceNow security operations team is also responsible for completing daily checklists across a range of security domains, including privileged account usage, IDS alerts, File Integrity Monitoring (FIM), and database access. The daily checklists and captured events are managed through a Now Platform instance. Any variances that are discovered are raised as incidents for tracking, notifications, and investigation.
Encryption

This section provides a high-level summary of the encryption capabilities of the Now Platform. More detail on these features can be found in Data Encryption.

Encryption in transit

Secure communication with the instance

Customer instances of the Now Platform are designed to be accessible via the internet, providing maximum flexibility on how, when, and from where they are accessed. The internet, however, is a public network and therefore communications can potentially be intercepted if they are not encrypted or otherwise protected.

Data in transit from a browser (normal user traffic) to the Now application is encrypted by default over TLS* (TLS 1.2 as a minimum) using AES (Advanced Encryption Standard) with 128-bit or 256-bit cipher suites.

Negotiated ciphers are subject to customer browser versions and may be influenced by customer internet proxy infrastructure. Customers can force specific cipher suites via their own browsers or proxies if desired, by a request of their required Cipher list via ServiceNow support.

All end-user access requests to a ServiceNow instance attempted over HTTP are redirected to HTTPS.

For additional security, customers can also use IP range-based authentication to restrict the public networks used to access their Now Platform instances.

The standard contractual clauses are applicable as a legal data transfer mechanism in the International Data Transfers section of the ServiceNow Data Processing Addendum.

Email in transit encryption

Customers commonly configure Now Platform instances to generate emails in relation to service management tasks, for example, to request approval for a change, or notify a user of the status of a service request.

Now Platform instances provide additional confidentiality in this respect by supporting opportunistic TLS for email sent or received. Now Platform instances will negotiate TLS (TLS 1.2 as a minimum) encryption during the SMTP handshake, including Sender Policy Framework (SPF), and will fall back to plaintext SMTP when a secure channel cannot be negotiated.

Additional related email security controls including Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) are also provided at no additional cost.

Integration encryption

Encryption can be applied to integrations such as LDAP and Web Services. Secure LDAP (LDAPS) connections require customers to provide certificates for their specific LDAP servers. Certificates may also be stored within an instance for use in signing of instance-bound web service requests.

Now Platform instances also support certificate-based mutual web services security authentication with external endpoints. FTPS and SCP can be used as file transfer methods to securely transfer data to their Now Platform instances. If desired, customers may also choose to use clear text protocols such as FTP or HTTP.

* References to TLS 1.2 include proposed TLS 1.3 suites, i.e., ECDHE-ECDSA (provides forward secrecy)
Encryption at rest and in use

Column Level Encryption (CLE)

Column Level Encryption (CLE) provides symmetric data encryption for supported data fields. Customers can select AES-128 or AES-256 encryption algorithms.

CLE is a free limited version of Column Level Encryption Enterprise (CLEE) available as part of the Platform Encryption and Vault security suites.

Platform Encryption subscription bundle

The Platform Encryption bundle comprises two encryption products that work together to meet most customers' typical needs:

1. Cloud Encryption encrypts all the data within the database at the Operating System layer.
2. Column Level Encryption Enterprise (CLEE) can then be used to encrypt selected fields or attachments within the application to ensure only authorized employees can access specific sensitive data.

Find out more details in Data Encryption.

Column Level Encryption Enterprise (CLEE)

Column Level Encryption Enterprise (CLEE) provide symmetric data encryption for supported data fields. Customers can select AES-128 or AES-256 encryption algorithms.

With a Column Level Encryption Enterprise subscription customers gain enhanced key management capabilities, a more flexible encryption policy, API support, and system-level access that enables automated processes and workflows to function on encrypted data.

Customers can provide their own encryption keys for CLEE, because it uses the Now Platform Key Management Framework (KMF).

Cloud Encryption (CE)

Cloud Encryption (CE) encrypts the storage volume that contains the customer's instance specific databases.

Cloud encryption also uses the Now Platform Key Management Framework (KMF).
**Edge Encryption**

Edge Encryption is an additional cost feature that uses a proxy application provided by ServiceNow (and installed by customer admins on their own network) that gives customers the ability to control the end-to-end encryption of their data and key management.

Edge Encryption encrypts supported fields and attachments inside a customer’s network using encryption keys stored and managed only within that customer’s network. Edge encryption also provides tokenization and substitution of data that matches standard data structures, such as credit card or social security numbers.

The data is encrypted from the moment it leaves the customer environment and that data is only decrypted by the proxy application (again within the customer environment) upon retrieval.

At no point is the data accessible in plaintext by ServiceNow systems or personnel.

### Key features of Edge Encryption

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Customer owned</strong></td>
<td>Customer-retained encryption key administration</td>
</tr>
<tr>
<td><strong>Flexibility</strong></td>
<td>Flexible encryption options to balance security and user operation requirements</td>
</tr>
<tr>
<td><strong>Tokenization</strong></td>
<td>Provides pattern-specific protection for structured data, such as credit card or Social Security numbers</td>
</tr>
<tr>
<td><strong>API support</strong></td>
<td>REST and SOAP APIs to support additional system integrations, web services, and customizations</td>
</tr>
<tr>
<td><strong>Easy administration</strong></td>
<td>Easily administer and rotate encryption keys</td>
</tr>
<tr>
<td><strong>Native platform</strong></td>
<td>Tight integration within the Now platform architecture to support ServiceNow applications and the ServiceNow portal interface</td>
</tr>
<tr>
<td><strong>Simple rule development</strong></td>
<td>A native encryption rule development environment to provide integration support</td>
</tr>
</tbody>
</table>

### Common use cases

- Requirements that prohibit encryption keys from being stored in a cloud service provider
- Mitigating the risk of exposing sensitive data as either the result of a direct attack or of compromised data stored in a cloud
- Customers who need to comply with governmental and industry certification requirements and regulations
- Addressing the data sovereignty requirement for data that may be stored outside of a country’s domain

The following diagram illustrates the Edge Encryption process where a field storing social security numbers (SSNs) is being encrypted within a customer’s network by an Edge Encryption proxy. The data in the SSN field is converted from plaintext to ciphertext.
Full Disk Encryption (FDE)

Full Disk Encryption (FDE) is an additional cost option that protects sensitive data from being exposed in the event of the physical theft of a drive used in a cloud instance, without impacting the application’s functionality.

FDE is a hardware-based approach that includes encrypting the entire disk, which can only be decrypted by the operating system. As such, FDE requires customers to have a dedicated hardware subscription.

FDE delivers at-rest protection only and focuses on preventing data exposure through the loss or theft of hard disks that hold customer data. To accomplish this, FDE uses AES-256-bit encryption for the physical drives and for the FIPS 140-2 Key Management System that supports them.

FDE decrypts the data when actively being used, or accessed, by the server’s operating system. The hard drive models used by ServiceNow comply with the Trusted Computing Group (TCG) enterprise specifications and are secured using a passphrase generated from a key stored in the ServiceNow Key Management System (KMS).

The most common use case for FDE is to provide an additional layer of security in cases where much (or all) of the data in the customer environment is considered sensitive (or could potentially be considered sensitive in the future), due to regulations or changes in the customer’s business environment.

Existing measures put in place by ServiceNow to mitigate the risk of loss or theft of storage devices may also be a factor when considering FDE.

FDE limitations
FDE does not provide application tier protection for data in transit, or against unauthorized access while the drive is operational.

Mobile application security

Mobile security
The native ServiceNow mobile applications for iOS and Android enable instances to be accessed from mobile devices. These apps support platform authentication using OAuth 2.0.

Authentication mechanisms include multi provider SSO, MFA, LDAP, Local DB, and Digest. ServiceNow mobile apps use an authentication methodology called AppAuth, which uses an external mobile browser to log the user in.

Once authenticated, mobile users are subject to the same access controls available on the Now Platform. Security information on these mobile applications, along with configuration best practices, can be found in the ServiceNow Mobile security overview.

Mobile application security controls
The ServiceNow mobile apps benefit from mobile-specific security controls, such as restricting clipboard operations, requiring a PIN for access, disabling attachments, and obscuring the app screen when in the background.

Data security
All data in transit is protected with TLS (TLS 1.2 as a minimum), and application preference information stored on-device is encrypted. By default, no data from an instance is stored on the mobile device.

Application distribution
The Now Platform mobile applications can be distributed with common Enterprise Mobility Management (EMM) or Mobile Application Management (MAM) applies customer’s corporate app protection policies to the mobile apps.
Conclusion

The ServiceNow environment supporting the Now Platform is a dedicated cloud, wholly owned and operated by ServiceNow. This infrastructure supports a multi-instance, logically single tenant architecture that enables isolation of customers from each other and provides real-time visibility of customer data location.

Key security benefits are provided through the Now Platform application including extensive automation, implementation of consistent global infrastructures, and standardized operational processes.

Customers can augment their instances with integrations to their own applications, services, and infrastructure as well as adopt built-in platform security features such as data encryption and network access control.

ServiceNow believes its customers are well-served by its application of relevant, measurable, and industry recognized information security frameworks. These include ISO/IEC 27001, 27017, 27018, and 27701, as well as accreditation with regional standards and regulations.

Transparent disclosure is another element of assurance available to all ServiceNow customers. This includes, but is not limited to, provision of the SSAE18 audit reports and ISO certificates.

For more information please reach out to your ServiceNow account team.

Additional Resources

- Cloud Security Customer Resources
- ServiceNow Trust Site
- ServiceNow legal schedules
- Product documentation
- Advanced High Availability white paper

"ServiceNow leverages Advanced High Availability architecture to transfer customers’ production instances between data centers when performing infrastructure maintenance such as patching, thereby minimizing the impact to availability."
## Appendix A: Edge Encryption options

<table>
<thead>
<tr>
<th>Operations</th>
<th>Standard AES-128 or AES-256</th>
<th>Equality-preserving AES-128 or AES-256</th>
<th>Order-preserving* AES-128 or AES-256</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES-128 or AES-256</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Group by</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Is empty</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Is not empty</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Equal</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Not equal (excludes empty fields)</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Is not</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Sort by</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is greater than</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Is greater than or equal</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is less than</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is less than or equal</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contains</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Starts with</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ends with</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operators that imply the right side of the clause is a field</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Text search</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* MySQL is required for order-preserving encryption
## Appendix B: Edge Encryption functionality & implications

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Implication</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reporting</strong></td>
<td>Reporting operates on column data values. Since the ServiceNow application must use the column’s values to generate reports, there is the potential a report will not generate correctly because it does not have access to the plaintext. This is only an issue if the report being generated uses columns that have been encrypted using Edge Encryption.</td>
<td>Review the columns that must be included in the report that may benefit from equality-preserving or order-preserving encryption, and use those supported functions where necessary. Do not export reports that contain encrypted columns, since the report is generated on a customer instance without access to the encryption key.</td>
</tr>
<tr>
<td><strong>Business rules and logic</strong></td>
<td>ServiceNow runs all business logic on the back end, so any business rule that needs to read from or write to an encrypted column may have trouble executing the rule.</td>
<td>Review the columns included in business rules that may benefit from equality-preserving or order-preserving encryption, and use those supported functions where necessary. If this is not possible, do not use the encrypted columns.</td>
</tr>
<tr>
<td><strong>Encrypted text exceeding table column widths</strong></td>
<td>Encryption algorithms often create ciphertext that is longer than the plaintext. For example, the name “King George III,” which is 15 bytes long, might be encrypted to “#j&amp;_ xz</td>
<td>[~`K@6_69FExN1$4n(2)c,” which is 30 bytes long. If the column in the ServiceNow instance is limited to 20 characters, the full length of encrypted text will not be stored, causing it to become invalid and incapable of decryption.</td>
</tr>
<tr>
<td><strong>Encrypted text exceeding table column widths</strong></td>
<td>Similar to business rules, workflows often operate from a column’s value. A workflow that depends on the ability to examine plaintext in a table column will fail to function because it only has access to encrypted versions of the text.</td>
<td>Customers should review the columns from their workflows that may benefit from equality-preserving or order-preserving encryption, and use those supported functions where necessary. If this is not possible, do not use the encrypted columns.</td>
</tr>
<tr>
<td><strong>Workflows</strong></td>
<td>Similar to business rules, workflows often operate from a column’s value. A workflow that depends on the ability to examine plaintext in a table column will fail to function because it only has access to encrypted versions of the text.</td>
<td>Customers should review the columns from their workflows that may benefit from equality-preserving or order-preserving encryption, and use those supported functions where necessary. If this is not possible, do not use the encrypted columns.</td>
</tr>
<tr>
<td><strong>Searching</strong></td>
<td>ServiceNow executes all searches on the back-end database, which means all searches use the data within the columns. If the search is being executed against columns with ciphertext values, rather than plaintext values, a user may not receive the desired results. However, searches for exact matches will still work because the search term will be converted into ciphertext by Edge Encryption – this only applies to equality-preserving and order-preserving encryption. This enables the back-end search function within ServiceNow to effectively search for the desired term. “Contains” searches on free-form text fields are the most difficult to implement because the search text cannot be found in the body of the encrypted text.</td>
<td>Tokenization can make “contains” searches possible. For example, a word or character string can be tokenized individually, so the encrypted search text finds a matching tokenized word in the body of the field. Equality-preserving and order-preserving encryption provide a technique that partially addresses the &quot;contains&quot; search with strong encryption.</td>
</tr>
<tr>
<td><strong>Sorting</strong></td>
<td>ServiceNow does all sorting on the back-end server. As an application, ServiceNow deals with large data sets and generally returns the Top N to the user based on some form of sorting. Because the application always sorts on the back-end, and the application always sorts on the ciphertext values, when a user initiates the sorting of encrypted data, the results may appear incorrectly.</td>
<td>Apply order-preserving encryption to implement a technique that addresses this issue (while maintaining strong encryption) using a stored subset of plaintext table data as a token to prepend to the ciphertext for sorting purposes before it is sent to the instance.</td>
</tr>
<tr>
<td>Functionality</td>
<td>Implication</td>
<td>Mitigation</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Bulk import/ export</td>
<td>ServiceNow does all export and import activities on the back-end servers. As such, any exported data — Excel, XML, CSV, PDF, or other exports the ciphertext values of any encrypted columns.</td>
<td>Some vendor solutions are capable of intercepting exported data files, such as XML or CSV, and decrypting them prior to being delivered to the user. Customers should check with their vendors to ensure that they can encrypt and decrypt the file types needed. If the desired file type can be encrypted, a web service integration is necessary.</td>
</tr>
<tr>
<td></td>
<td>Likewise, because these data formats are not supported, any attempt to import data into an encrypted column will result in unencrypted values being written into the column, unless the process that is sending data to the instance is configured to proxy communications through the Edge Encryption proxy.</td>
<td></td>
</tr>
<tr>
<td>Mobile access</td>
<td>To see any data that has been encrypted using Edge Encryption, a mobile browser must access the ServiceNow instance through the Edge Encryption proxy. Actions allowed via mobile devices need the ability to see the plaintext data for the ServiceNow application to function correctly. This includes workflow approvals via mobile devices and other actions available to the user through the mobile interface.</td>
<td>Ensure that mobile access to the ServiceNow instance goes through the company’s network so all access is granted via the Edge Encryption proxy. Be selective about which columns</td>
</tr>
<tr>
<td>Inbound/ outbound email and SMS notifications</td>
<td>When ServiceNow triggers a notification, it could send an email or SMS that contains a mixture of hard-coded plaintext and encrypted field text. For example, an email template can be rendered with field substitutions that looks like this: Dear ${name}, we have changed your shirt size from ${old_size} to ${new_size}. If the corresponding columns are encrypted the email looks like this: Dear Bob Baker, we have changed your shirt size from $6^SD[&amp;%T$ to $H7asdh78$.</td>
<td>Edge Encryption does not support inbound or outbound email. Taking this into account, customers should be selective about which columns they encrypt. Modify any SMS text message that uses encrypted columns and remove them from the message. Provide a URL in the message that leads to a ServiceNow page that shows the contents of the message—this way, the Edge Encryption proxy can decrypt the text.</td>
</tr>
<tr>
<td>Reference fields</td>
<td>Reference fields are not supported by Edge Encryption because the sysid that is being used to make the link between the customer’s form and the actual field needs to be in the clear.</td>
<td>Use a secondary field, encrypt it, and hide the reference from the form. The actual source field must be a string type and will need to be</td>
</tr>
<tr>
<td>Web services integrations</td>
<td>ServiceNow can integrate with outside data sources using industry-standard web service protocols like REST and SOAP. A third-party integration, which is usually software running on a computer inside a customer’s network, can retrieve and insert data into ServiceNow automatically, but if that data is not properly encrypted, plaintext can be inserted into columns that are expected to be encrypted. As a result, the Edge Encryption proxy attempts to decrypt text that was not encrypted in the first place. This leads to data inconsistencies within the ServiceNow instance and could impact what the user sees.</td>
<td>Configure all automated processes to send or receive data from the ServiceNow instance using encryption rules so the Edge Encryption proxy can identify the columns in the payload with the encrypted instances.</td>
</tr>
<tr>
<td>Legacy data</td>
<td>ServiceNow customers may have amassed large amounts of data within their ServiceNow instances within various columns. The amount of data these customers need to encrypt could contain millions of records. Because encryption keys and algorithms cannot be held within ServiceNow, encrypting large amounts of data using Edge Encryption can take a long time.</td>
<td>Customers can run a mass encryption job on a per-column and attachment basis. This type of operation should be planned operation carefully so that customers can accommodate for the volume of columns and attachments they plan to encrypt.</td>
</tr>
</tbody>
</table>