Securing the Now Platform
An overview of the ServiceNow security program
Introduction

ServiceNow® provides a cloud-based platform and solutions that deliver digital experiences and help people do their best work. Our applications automate, predict, digitize, and optimize business processes and tasks across the enterprise.

Having a single product, platform, and support infrastructure means that ServiceNow can employ extensive security without the need to balance security over a highly diverse estate.

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 data layers. In addition to the security features that come as standard within the platform, customers can leverage additional security capabilities within their ServiceNow instance(s).

This document describes ServiceNow’s security program across a number of key physical, administrative, and logical security domains. These include 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.

Please note, all information in this eBook is related to the standard Now Platform commercial environment. For information related to ServiceNow’s in-country cloud offerings around the globe and how they may differ, please contact your ServiceNow account representative.
Distributed denial of service (DDoS) ................................................................. 21
Vulnerability management ..................................................................................... 21
Now Platform vulnerability management .............................................................. 21
Cloud infrastructure vulnerability management ................................................... 21
Instance Integrations ............................................................................................ 22
Overview of instance integrations ....................................................................... 22
ServiceNow MID Server ..................................................................................... 22
Web services integration ..................................................................................... 23
Now Platform malware protection ...................................................................... 23
Instance communication hierarchy ...................................................................... 23
Accessing Data ..................................................................................................... 24
Customer access to data ..................................................................................... 24
ServiceNow access to customer data .................................................................. 24
Authentication and authorization ....................................................................... 24
Authentication ...................................................................................................... 24
Authorization ........................................................................................................ 25
Customer access management .......................................................................... 25
High security settings plugin ............................................................................. 26
Security logging and monitoring ......................................................................... 26
Overview of logging and monitoring ................................................................. 26
Logging and monitoring ServiceNow instances ................................................ 27
Logging and monitoring ServiceNow security infrastructure .......................... 27
Encryption .......................................................................................................... 28
Encryption overview .......................................................................................... 28
Encryption key management overview .............................................................. 29
Mobile application security ................................................................................ 30
Mobile security ................................................................................................... 30
Conclusion ........................................................................................................... 31
Definitions

The ServiceNow environment is a private enterprise cloud service, fully owned and operated by ServiceNow. This cloud features a multi-instance architecture that delivers logical single tenancy by isolating all customers’ data from each other. This is achieved by utilizing an enterprise-grade cloud architecture and a dedicated database and application services per customer instance, ensuring that there is no possibility of co-mingling of 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 worldwide 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. Further information regarding the Now Platform can be found here.

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. Production instances are automatically replicated to passive data centers, whereas sub-production instances only exist in a single data center.

Security responsibilities

Data roles and responsibilities

As the ‘data controller,’ customers always retain ownership of their data and are therefore responsible for meeting the requirements of privacy legislation in the jurisdictions in which they operate and from which they collect personal data. If an individual requests information directly from ServiceNow regarding data that may be stored about them on the Now Platform, ServiceNow will always refer that individual to 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 it is being used in accordance with those conditions.

Regardless of how customers classify data that is stored in their instance, ServiceNow’s single operating and security model ensures that 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 on the next page. For more information about security responsibilities with respect to customer data, please review Safeguarding Your Data.
<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>Data management (classification and retention)</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>Authentication and authorization</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 flight</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>Vulnerability management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business continuity and disaster recovery</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>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>Infrastructure management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure configuration of instance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee vetting or screening</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environment controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical security</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Information security governance and risk management**

**Security frameworks**

ServiceNow’s security framework is based on ISO/IEC 27002:2013. As an ISO/IEC 27001 certified organization, there is a high level of integration between the ISO/IEC 27002:2013 code of practice and the ServiceNow information security management system (ISMS). ServiceNow has been an ISO 27001 certified organization since 2012 and is also ISO/IEC 27017:2015 and 27018:2014 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 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.
Security policy, standards, and procedures

ServiceNow's security program is described in its information security management system (ISMS) and associated security policies and standards. These are reflected in an extensive library 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’s 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 in the case of significant changes or at least every two years by a managed program.

Security management

ServiceNow’s 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, creating documentation, and 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. Regular assessments are performed to identify and assess the likelihood and impact relating to risks. These risks can include those regarding 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, and any identified risk is quickly and efficiently managed in a timely manner in order 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, and 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 and comprehensive review.

At a minimum, quarterly entitlement reviews are carried out to ensure that personnel have the appropriate logical and physical access rights are assigned to them. This includes those responsible for management of its 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. This is used both for new requests and reassignment of access for existing personnel. This approach mitigates potential incorrect assignment of access, which can occur where 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 further 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 & 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 (GSAT) training, and fulfillment of training requirements is measured and enforced. The content of the training varies from year to year, as different security topics, risks, threats, and requirements are identified. Some examples are listed below:

- Privacy and data protection
- Code of conduct and ethics
- Insider trading and foreign corrupt practices
- Email and instant messaging
- Physical security
- Cloud technologies

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 using ServiceNow’s 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 and in line with the principle of least privilege. Regular entitlement reviews are conducted to ensure that the processes are working and to remediate any changes or removals that have not been processed appropriately. Employees exiting ServiceNow have all access removed within a maximum period of 24 hours.

Compliance

Why certification matters

Every year ServiceNow is rigorously audited by independent third-party companies and government bodies to prove that we comply with various global and regional standards governing information security. Each audit represents not just a ‘tick in the box’, but a significant commitment and ongoing effort; each one involves thousands of point-in-time and ongoing assessments covering every aspect of our information security program and efforts.

Our accreditors are experts in their respective fields with a deep understanding of the different global and regional laws and standards that must be complied with. They
thoroughly assess ServiceNow’s processes and controls against these standards, verifying that they are met or exceeded at all times. When the audit reports are complete, we make them available to customers.

All of this means that customers can be confident that ServiceNow consistently demonstrates excellent security controls and practices. It reduces the need for customers to generate and assess large quantities of detailed questions on these topics, as multiple well-qualified, independent assessors regularly do this on their behalf.

A note about GDPR

The General Data Protection Regulation (GDPR) is not listed below because GDPR is not a standard—it is a regulation, i.e. a law, and ServiceNow complies with the law in all jurisdictions in which it operates. ServiceNow has found transition to GDPR compliance a relatively pain-free process. It is not yet possible to achieve certification against GDPR, but ServiceNow will consider that in future should it become possible.

Regulatory and industry compliance

ServiceNow has a dedicated audit, risk, and compliance (ARC) team responsible for a number of governance and compliance efforts across the organization, including managing ServiceNow’s compliance program. This requires engagement across multiple functional areas within ServiceNow, including legal, finance, and procurement. ServiceNow’s legal organization engages both internal and external legal counsel to understand ServiceNow’s obligations to existing and new laws and statutory regulations within the jurisdictions in which it operates. The finance department is responsible for ensuring ServiceNow’s compliance with relevant financial regulations, including Sarbanes Oxley (SOX), a requirement for all US public companies.

ServiceNow itself is not subject directly to vertical-specific regulation, such as HIPAA, PCI, or NERC-CIP; however, it does have many customers who are. And through the features in the Now Platform and organizational transparency, it can support those regulated customers in meeting their obligations.

In addition, ServiceNow operates a quality management system (QMS) based on the ISO 9001 standard. The ServiceNow has a dedicated QMS team, quality engineering team, and compliance team to ensure continual improvement. The table below summarizes ServiceNow’s security-related certifications.

<table>
<thead>
<tr>
<th>Certification or attestation</th>
<th>Description</th>
<th>Geography</th>
<th>Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC 27001:2013</td>
<td>Specifies information security management best practices and controls</td>
<td>International</td>
<td>All</td>
</tr>
<tr>
<td>ISO/IEC 27017:2015</td>
<td>Implementation of cloud-specific information security controls</td>
<td>International</td>
<td>All</td>
</tr>
<tr>
<td>ISO/IEC 27018:2014</td>
<td>Securing personally identifiable information (PII) in the cloud</td>
<td>International</td>
<td>All</td>
</tr>
<tr>
<td>ISO/IEC 27701:2019</td>
<td>Establishing, implementing, maintaining, and improving a Privacy Information Management System (PIMS)</td>
<td>International</td>
<td>All</td>
</tr>
<tr>
<td>SSAE 18 SOC 1 and SOC 2 Reports</td>
<td>SOC 1 Type 2 focuses on protecting the confidentiality and privacy of information in the cloud that affects the financial reports of customers. SOC 2 Type 2 focuses on controls that are relevant to security, availability, processing integrity, confidentiality, or privacy</td>
<td>International</td>
<td>All</td>
</tr>
<tr>
<td>Certification or attestation</td>
<td>Description</td>
<td>Geography</td>
<td>Industry</td>
</tr>
<tr>
<td>------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>SSAE 18 SOC 2 + HITRUST Report</td>
<td>Provides a mechanism for the service auditor to opine on the design and effectiveness of the Trust Services Criteria and the HITRUST CSF in the same report.</td>
<td>International</td>
<td>All</td>
</tr>
<tr>
<td>FedRAMP JAB High P-ATO (for US government entities)</td>
<td>US government-wide program that provides a standardized approach for assessing, monitoring, and authorizing cloud computing products and services</td>
<td>United States</td>
<td>US federal government/DoD</td>
</tr>
<tr>
<td>DoD Impact Level 4 Authorization (for US DoD/IC entities)</td>
<td>US government baseline for security requirements for cloud service providers that host DoD/IC information</td>
<td>United States</td>
<td>US federal government/DoD</td>
</tr>
<tr>
<td>APEC Privacy Recognition for Processes (PRP)</td>
<td>Certifies the adoption of sound risk management and security practices for cloud companies</td>
<td>International</td>
<td>All</td>
</tr>
<tr>
<td>ASD Certified Cloud Service</td>
<td>Helps Australian government agencies effectively engage and consume cloud-based solutions.</td>
<td>Australia</td>
<td>Australian federal government</td>
</tr>
<tr>
<td>Multi-Tier Cloud Security Standard for Singapore (MTCS) Level 3</td>
<td>Certifies the adoption of sound risk management and security practices for cloud companies</td>
<td>Singapore</td>
<td>All</td>
</tr>
<tr>
<td>BSI Cloud Computing Compliance Controls Catalog (CS)</td>
<td>Cloud-specific compliance controls catalog developed by the German Federal Office for Information Security (BSI).</td>
<td>Germany</td>
<td>All</td>
</tr>
<tr>
<td>Government of Canada Cloud Provider</td>
<td>The Canadian Centre for Cyber Security (CCCS) defined data classification level that is approved to be stored within the cloud.</td>
<td>Canada</td>
<td>Canadian federal government</td>
</tr>
<tr>
<td>Cyber Essentials Plus Certification</td>
<td>UK government certification for risk mitigation and assessment of cyber security threats to IT systems.</td>
<td>United Kingdom</td>
<td>All</td>
</tr>
</tbody>
</table>

**Physical and logical architecture**

**Overview of physical architecture**

ServiceNow’s physical architecture supporting its private cloud is deployed into dedicated, ServiceNow–managed colocation.
spaces and is implemented globally. In these locations, ServiceNow’s own 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. Where supported, some data centers also feature electrical supply resilience across multiple grid suppliers.

**Infrastructure operations management**

As a cloud service provider (CSP), a significant element of ServiceNow’s responsibilities is to provide and manage the underlying infrastructure on which instances of its Now Platform are deployed. A number of complementary activities and processes are undertaken in managing this environment, all using ServiceNow’s own products.

---

**Capacity management**

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

**Configuration management**

Continuous monitoring is undertaken to validate the configurations for each of the system and application components that make up 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 hundreds of changes a week and thousands of changes each month.

---

**Global data center pairs**

ServiceNow’s data centers are arranged in pairs. There are nine support centers and 13 high availability data center pairs, spanning five continents: Asia, Australia, Europe, North America, and South America.

All customer production data is stored in both data centers 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.

There are also pairs exclusively for qualified US Federal and Swiss banking customers. 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 (DC) pairs, where both members are either within the same jurisdiction or within mutually compatible jurisdictions so that even when data is transferred from one DC to another, the sovereignty of the data is preserved.

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

**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 27001:2013 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; these include public, internal, power, environmental, UPS and battery rooms, loading bays, and other zones. Although the detail of the zones will vary between the data centers, the principle is applied across them all. Access controls are applied to prevent movement of unauthorized data center staff between each zone in the data center.

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

Data center access control systems prevent staff from entering any area in which 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).

Personnel access control

Logical access to the infrastructure hosting the ServiceNow cloud and all hosted customer data is granted only to ServiceNow personnel with the specific requirement to do so. Access where required is provided on a per-role basis, according to specific job functions and a least-privilege model and reviewed regularly.

In accordance with separation-of-duties good 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. The private cloud environment is both physically and logically isolated from ServiceNow’s corporate environment and is also subject to different standards, policies, and governance reflecting its different purposes and dispositions. To manage the private cloud infrastructure, 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, from which employees cannot extract or copy data. Host-based data leak prevention (DLP) is enabled, SSH access to production servers is controlled using a proxy, and all user activity is controlled and monitored with a privileged access management (PAM) system.

ServiceNow does not outsource any service, operational, or management functions that would provide any third party with access to systems hosting customer data or to customer data itself. ServiceNow limits the infrastructure supporting its cloud’s footprint to only those technologies, infrastructure, and components required to support the Now Platform.

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 on a regular basis.

Electrical and environmental controls

ServiceNow’s data centers are highly available facilities with redundant electrical and mechanical systems. While not formally accredited, the data centers are designed to operate equivalently to a minimum of the TIA942 Tier 3 standard.

Electrical systems
ServiceNow’s data center providers typically offer between 99.999% and 100% power uptime. 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. These data centers can typically operate for at least 24 hours at full electrical load without the requirement of additional fuel. 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. Uninterruptable power supply (UPS) is provided either by battery or flywheel systems that can sustain systems until generators can be activated.

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.

Overview of logical architecture
ServiceNow’s highly defined and limited environment allows for a number of key benefits:

<table>
<thead>
<tr>
<th>Automation</th>
<th>Support, scalability, security</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 and expected outcomes, and reduces the potential for, and impact of, human error.</td>
<td>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 ServiceNow 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 and instance of the Now Platform.</td>
<td>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.</td>
</tr>
</tbody>
</table>

![Logical Architecture Diagram](image-url)
Internet services layer (proxy layer)

Customers and web services connect to the ServiceNow private cloud over HTTPS using TLS for communication to and from a ServiceNow 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 ServiceNow instances. However, for additional convenience, ServiceNow offers native mobile apps for iOS and Android.

The proxy layer forwards requests made 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 performed in this tier.

Application layer

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

ServiceNow instances are the termination point for all inbound requests made by end users of those instances. 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.

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 ServiceNow instance.

Each instance has a single database present on a database server running multiple discrete and segregated database services. There is no comingling 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 ServiceNow’s architecture is that it creates a very distinct logical boundary between the data of each customer, which 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.

ServiceNow’s unique multi-instance 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 any
time. Knowing exactly where all of a customer’s hosted data is located also enables ServiceNow to reliably and securely delete that customer’s data in its entirety, if required.

The multi-instance tenancy model also facilitates:

- 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; and
- the ability to perform upgrades and maintenance on an individual basis without impacting other customers’ instances, enabling exceptional instance availability.

Availability

ServiceNow provides a highly available cloud infrastructure through its Advanced High Availability (AHA) architecture.

Advanced high availability (AHA) overview

ServiceNow’s 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’s data centers are arranged in pairs, with all customer production data hosted in both data centers simultaneously and 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.

We leverage 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 the 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 part of our standard operating procedures. This ensures that when it is needed to address a failure, the transfer will be successful and service disruption is minimized.

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 and always coordinated with a customer. These outages occur within the contracted availability service level agreement that ServiceNow commits to with its customers.
**Failover**

A failover of an instance is an event usually performed where availability for one or more customer instances cannot be maintained. This could be down to 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. Where 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 centers, these times are usually 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 are employed to provide robust, resilient name resolution services.

**Data backup and recovery**

ServiceNow’s 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. Such circumstances could be, for example, where a customer deletes some data inadvertently, or where 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 capability would not assist and restoring from backup is the only option for recovery.

Full backups are performed every seven days direct to disk and are retained for 28 days, with differential backups taken every 24 hours. 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 made within both data centers in a pair, therefore benefiting from geographic separation.

Backups are encrypted with AES-256 using randomly generated encryption keys for every backup. These are kept in a secure key store. And it is 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, given the maximum 28-day backup retention period. 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, as required.

**Business continuity and disaster recovery**

ServiceNow is divided into two distinct environments for the purposes of business continuity (BC) and disaster recovery (DR). ServiceNow’s corporate IT environment and its cloud data centers are both physically and logically isolated from each other. A disaster affecting ServiceNow’s corporate environment could occur with little or no impact on the ability for the data centers within the private cloud 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.

**Cloud continuity**

**Execution**

ServiceNow’s Information System Contingency Plan (ISCP) covers its cloud data center environments. Its 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 ServiceNow’s 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**

ServiceNow’s 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.

**Software development: Security by design**

**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 into 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**

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 in respect to new features security features
- Curating educational security materials, including those for customers
**Application security testing**

ServiceNow's 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 within ServiceNow using a variety of methods. Third-party commercial and in-house automated toolsets, including static and dynamic application security testing, are used as well as manual testing and peer code reviews. These efforts are all specifically in relation to 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 ServiceNow's secure development practices. A third-party organization is given an extended period of time and access to the resources necessary to review and test the next release of the Now Platform before it is made available to customers.

On completion of a first round of testing, any confirmed issues are entered into the ServiceNow problem resolution process, prioritized, and categorized. Those whose impact and criticality meet pre-defined ServiceNow criteria are remediated prior to any re-testing.

Once the remediation completes, a second round of testing is conducted again by the same third-party organization. This is in order 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 Compliance and Operational Readiness Evidence (CORE) portal.

**Customer application penetration testing**

Another significant aspect of ServiceNow’s application penetration testing program involves tests performed by its customers on their own ServiceNow instances, in accordance with a documented process. Customers are permitted to perform one penetration test per year.

Scheduling of testing must be pre-approved and conducted at a date and time agreed with ServiceNow. This is necessary to allow ServiceNow to continue to conduct its monitoring activities and be able to differentiate potential attacks from authorized customer testing.

As a prerequisite to carrying out testing, customers must upgrade their instances to the latest release and patch version and implement ServiceNow’s hardening guide. Testing without these prerequisites would likely result in false positive identification of previously identified issues. As a further condition of testing, customers are also required to share their testing scenarios for any findings from their test, along with their overall results with ServiceNow.

Confirmed customer findings help contribute to the collective security of the ServiceNow environment and enable a continuously improving security posture, and the customer penetration testing scheme 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 ServiceNow’s vulnerability management criteria.

The release notes on the ServiceNow docs site for each major version, patch, and hotfix include information regarding what has been remediated in each release, including those that are security-related.

**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 ServiceNow instance and should therefore apply access controls according to their data classification policies.

**Data retention**

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.

Data that is deleted from a customer instance will remain backed up for 28 days before it is permanently deleted.

**Media disposal**

ServiceNow hosts its customer data on solid-state drives (SSD) or mechanical disks 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 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 datacenter 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 ServiceNow instance. This can be via the UI interface through integrations or by using optional ServiceNow components, such as the free ODBC connector or MID Server.

Upon contract expiration or exit, or where requested, ServiceNow will supply a customer’s data in an SQL dump format. Exiting customers have 45 days to request their data to be returned, after which all hosted and backed-up data is automatically deleted and overwritten.

**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 daily for public facing infrastructure on an unauthenticated basis. Weekly scans are 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, and all relevant services and system components send security logs and events to a SIEM for security monitoring and alerting. See ‘Security 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. This includes 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 new ServiceNow Patching Program. Each quarter, one full patch and two security patches will be automatically scheduled to update your instance(s).

An instance of ServiceNow 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 where 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 ServiceNow’s vulnerability management tools are automatically logged within an internal ServiceNow instance. These are first reviewed by ServiceNow personnel to determine that the appropriate level of priority is assigned, taking into factors such as relevant mitigating controls and exposure. Those issues identified at the highest risk classification level will be targeted for remediation as quickly as possible.

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

Once it is determined 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. Where no clear remediation is available virtual patching is implemented.

ServiceNow leverages the 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.

ServiceNow does not condone any attempts to actively audit our infrastructure. However, we recognize that vulnerabilities in our systems, products, or network infrastructure are occasionally discovered incidentally. If customers discover a vulnerability, they should report it 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 programmatically or through the use of features in the Now Platform, including IntegrationHub, to simplify and accelerate customer integrations.

Additionally, the platform offers a rich interface for loading external data using import sets. Using this feature, customers can load from various data sources such as HTTPS, FTPS, and SCP using file formats such as XML, CSV, and Microsoft Excel XLS files. Information can also be pulled from a data source using a direct JDBC connection, provided customer network connectivity permits it.

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

Information within an instance can be exported and migrated to an external platform using an open database connectivity (ODBC) driver that’s 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.

### ServiceNow MID Server

The ServiceNow management, instrumentation, and discovery (MID) Server is an optional, free ServiceNow component. It facilitates communication of data between the customer instances and external applications, data sources, and services. MID Servers are used by customers 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. It may be installed by the customer on a suitable host system within their environment. The server can use Windows or Linux operating systems. MID Servers are cryptographically paired with an individual instance during installation and need to be approved by the customers ServiceNow administrators before they 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 1.2, looking for activities to perform. The activity is 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.

A ServiceNow instance provides a customer with a number of authentication options that can be used simultaneously within an instance, using a multiple authentication model.
Web services integration

ServiceNow supports web services using SOAP (Simple Object Access Protocol) and REST (Representational State Transfer) for integration, all traffic is encrypted using TLS.

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

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 ServiceNow instance.

ServiceNow instances support outbound-only web services mutual authentication by defining a protocol profile for connections that require mutual authentication. Protocol profiles allow you to associate a specific certificate record with a protocol, such as HTTPS. Requests made to an endpoint whose domain is defined in a profile are then mutually authenticated.

Mutual web services authentication is only possible for outbound HTTPS connections, such as SOAP, REST, or direct HTTPS calls. A ServiceNow instance does not support mutual authentication for inbound requests or for outbound requests sent through a MID Server.

Secure signing of SOAP requests for message integrity purposes is also available.

Now Platform malware protection

Now Platform instances feature antivirus protection to protect 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 ServiceNow instances over HTTPS from any endpoint device with a browser, or from a system or application level integration.

An instance itself 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 on customer direction. These are via activities they define 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 necessary to support any network topology ranging from a flat to a highly segmented network.
Accessing Data

Customer access to 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. In general, ServiceNow does not access customer data, but it is sometimes necessary during the course of resolving customer support tickets.

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

Only members of ServiceNow’s support organization who have been specifically assigned to an active incident 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 that access is requested.

Access can only be gained via a secure virtual desktop environment accessible only from ServiceNow data centers, requiring 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 enabled, SSH access to production servers is controlled using a proxy, and all user activity is controlled and monitored with a privileged access management (PAM) system.

More information regarding access control can be found in Data Access Controls.

Authentication and authorization

Authentication
A ServiceNow instance provides a customer with a number of authentication options that can be used simultaneously within an instance, using a multiple authentication model.

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

The ServiceNow 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 that are compliant to the SAML 2.0 standard.

Customers who implement their own SAML compliant IdP or opt for a third-party service can then also 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.

Lightweight Directory Access Protocol (LDAP)
LDAP authentication lets 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 these. A directory needs to be accessible to the relevant ServiceNow instance because 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 commence with end users providing their username and password to the customer’s ServiceNow 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 ServiceNow instance. As part of the LDAP integration, passwords are neither stored nor transferred back to the customer’s ServiceNow instance.
Built-in “native” authentication

In the case of native authentication, passwords are managed solely by customers within their ServiceNow instance(s). This is the only authentication method where both the username and password are stored within a customer’s instance (as a 1-way SHA-256 hash with an appropriate salt value).

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

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:

- Auth external client scenario
  A customer’s instance provides an endpoint for third-party clients to pull data from the instance.

- Auth provider scenario
  A customer’s instance pulls data from a third-party provider.

Authorization

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

A ServiceNow instance includes a built-in role-based access control (RBAC) mechanism providing user, group, and role objects. These can be used by customers to assign access to applications and data within their instances. Customers 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 ServiceNow instance. Customers can add to those per their own requirement.

ACLs comprise 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 users. 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 ServiceNow instance(s).

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), and the entitlements and access levels granted to those users.

User identity synchronization

A ServiceNow instance requires 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 for role-based access purposes.

To facilitate this requirement, ServiceNow instances support both automated and manual creation of user identities. This includes synchronization of users, their group memberships, and those 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. This then allows synchronizing the information in customers’ ServiceNow instances with that in their own directory service. Customers specify the interval or regularity of synchronization per their own requirements. This would usually be 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 ServiceNow 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 from where it can access the directory server and return a payload of users or groups and their attributes to the customers’ instance. These would then be automatically imported or updated in the target user or group tables within the instance.

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

If a user exists in a customer’s IdP but is not in the customer’s ServiceNow instance, SAML user provisioning can automatically create the user in the instance.

High security settings plugin

ServiceNow’s High Security Settings plugin provides advanced security options for instances of ServiceNow and is enabled in all new instances. This plugin cannot be disabled. Security features enforced by the plugin includes the ‘default deny’ access mode, enables access control rules, and provides elevated access functionality and security-related roles for a customer’s administrators.

The settings also include a number of out-of-the-box security-related properties. Customers may 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. Advice and guidance can be found in ServiceNow’s Security Best Practice Guide on the Now Support Service Portal and the Instance Hardening Settings on ServiceNow Docs.

Security logging and monitoring

Overview of 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 ServiceNow instance or exported to a customer’s security information and event management (SIEM) tool. Workflows or incidents can be automatically created based upon 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.

ServiceNow collects and retains logs and events relevant to its entire cloud infrastructure, including information regarding requests made to instances of the Now Platform in order to detect potentially malicious actions or activities in relation to its service. 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 ServiceNow instances. However, events that occur within a specific customer’s instance are accessible to that customer through their instance logs. These events are also captured in ServiceNow’s 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>
</tbody>
</table>
### Log type

<table>
<thead>
<tr>
<th>Log type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 ServiceNow instances

A ServiceNow instance generates detailed log and audit information regarding activities which take place within it. ServiceNow’s default application logging capabilities 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. Customers manage and monitor the various 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 for log and audit events to be stored within a customer’s environment and retained according to the customer’s specific requirements.

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 problem, or any one of a number of standard, pre-configured events. They may also be extended to contain customer defined events. A number of security-related events are also available in the event log. These include those recording successful login, failed login, security privilege escalation, and viewing of tables or records.

In addition to reviewing logs manually, workflows or actions can execute 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 be to issue 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 relates to recording all activities in respect to data and customizations within customer instances. 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 of any 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. ServiceNow’s incident response process includes event discovery, triage, escalation, notification (including customer notification), remediation, and post-mortem review.

If a customer’s environment or data is impacted, the customer will be notified without undue delay. Contractual commitments can...
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 ServiceNow’s 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 pre-defined triggers and metrics. These are reviewed by a 24/7 security operations capability with global coverage.

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

Events, alerts, and relevant logs are also fed from other systems, including all servers, network devices, and ancillary systems into the SIEM. 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 ServiceNow 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 to ensure good separation of duties.

Network traffic log events are retained for a minimum of 90 days, whereas infrastructure events are retained for one year.

ServiceNow’s 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 ServiceNow instance. Any variances that are discovered are raised as incidents for tracking, notifications, and investigation.

Encryption

Encryption overview

ServiceNow provides all enterprise customers with encryption for data in transit. Optional features for encryption of data at rest are also available and may be applied or layered as needed. This section summarizes encryption capabilities at a high level; details that describe these features can be found in ServiceNow’s Data Encryption eBook.

Encryption in transit

ServiceNow customers access their instances over the internet using Transport Layer Security (TLS) encryption using AES 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. All end-user access to a ServiceNow instance attempted over HTTP are redirected to HTTPS.

Encryption at rest

ServiceNow instances provide customers with optional mechanisms to implement encryption for data at rest.

Platform and column encryption

Platform encryption and column encryption provide symmetric data encryption for individual supported data fields. Customers may select AES-128 or AES-256 encryption algorithms and may optionally provide their own encryption keys.
• Fields in the instance with a ‘system’ flag or those used in customer workflows and automation cannot be encrypted.
• Data stored in fields encrypted with this feature cannot be filtered or sorted.

Platform encryption uses ServiceNow’s Key Management Framework (KMF). Compared to Column encryption, this allows enhanced key management capabilities, more flexible encryption policy and API support.

**Edge encryption**

An additional cost feature that performs data encryption inside a customer’s network using encryption keys stored and managed only within that customer’s network. Supported fields and attachments may be encrypted. Encryption takes place via a proxy application installed inside a customer’s network that functions as a cloud access security broker (CASB).

When using this feature, unencrypted target data is never stored in a customer’s ServiceNow instance. Edge encryption also provides tokenization and substitution of data that matches standard data structures, such as credit card or social security numbers.

**Database encryption**

Database encryption encrypts all customer data at rest in the database with no impact to functionality. It uses the native capabilities of the database engine to encrypt data as it is written to the database and decrypt as it is read from the database using AES-256-encryption. When using database encryption, all data is encrypted, including attachments, logs, and backups. ServiceNow applications (including custom applications) can operate seamlessly because the application always has access to the unencrypted data.

This technology, often called “tablespace encryption” or “transparent data encryption,” is fully transparent to the customer and to the application.

**Full disk encryption**

An additional cost feature that provides encryption for data at-rest only is available through self-encrypting hard drives. This also requires the purchase of dedicated ServiceNow hardware at further additional cost. AES-256-bit encryption is implemented in these devices and in the key storage appliances that support them.

Full disk encryption is solely intended to mitigate the risk of data exposure through the loss or theft of physical storage devices used for customer data.

Wherever possible, ServiceNow leverages FIPS 140-2- certified technologies in its federal environment.

**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.

ServiceNow 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 ServiceNow instances. If desired, customers may also choose to use clear text protocols such as FTP or HTTP.

**Email in-transit encryption**

Customers commonly configure ServiceNow 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. ServiceNow instances provide additional confidentiality in this respect by supporting opportunistic TLS for email sent or received. Now Platform instances will negotiate TLS 1.2 encryption during the SMTP handshake and will fall back to plaintext SMTP where a secure channel cannot be negotiated. Additional related email security controls including Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) are also provided at no additional cost.

**Encryption key management overview**

**Platform encryption**

Platform encryption differs from column encryption in that it uses ServiceNow’s Key Management Framework (KMF). The KMF
provides enhanced key management capabilities following NIST 800-57 guidelines and allows customers to provide their own keys. Customer keys are re-encrypted (wrapped) with multiple higher-level keys, with the root key being stored in a FIPS 140-2-L3 compliant Hardware Security Module (HSM) within the ServiceNow cloud infrastructure.

**Column encryption**

Encryption keys are backed up within the database for the customer instance where they are used. Both instance-generated and customer-supplied keys are re-encrypted using a wrapper key which is securely stored in a ServiceNow-managed HSM within the ServiceNow cloud infrastructure.

**Edge encryption and database encryption**

Encryption keys for the Edge encryption feature are managed entirely within a customer's network boundary. Encryption keys for database encryption are managed by ServiceNow using a three-level key hierarchy. The first two keys are customer-specific and are created by the database engine, while the third key is instance-specific.

**ServiceNow cloud infrastructure**

Encryption keys used within ServiceNow's cloud infrastructure are managed by ServiceNow. Keys are stored in redundant secure key storage appliances. Dual controls are required for essential functions such as generating, deleting, or exporting keys. Key custodian forms are required as part of the generation of new keys. Cryptographic management is undertaken by a specific team within the security group, including appliances used to store the per customer instance wrapper key.

**Mobile application security**

**Mobile security**

The native ServiceNow mobile applications for iOS and Android enable instances to be accessed from mobile devices. These apps use the same robust authentication mechanisms available in instances of the Now Platform. Once authenticated, mobile users are subject to the same access controls.

**Mobile application security controls**

The 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, and application preference information stored on-device is encrypted. By default, no data from an instance is stored on the mobile device.

**Application distribution**

ServiceNow's mobile applications can be distributed with common enterprise mobility management (EMM) or mobile device management (MDM) platforms.
Conclusion

The ServiceNow environment supporting the Now Platform is a dedicated cloud, fully 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 application of extensive automation, implementation of a 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.

Finally, ServiceNow believes its customers are well-served by its application of relevant, measurable, and industry recognized information security frameworks. These include ISO/IEC 27001:2013, ISO/IEC 27017:2015, and 27018:2014, as well as accreditation with regional standards and regulations. Transparent disclosure is an additional element of assurance available to all customers. This includes, but is not limited to, provision of the SSAE18 audit reports and ISO certificates.

For further information on ServiceNow, visit www.ServiceNow.com or contact your account representative.