

# Securing the Now Platform

The ServiceNow security program overview

## Definitions and context

Information security governance and risk management

Privacy and regulatory compliance

Architecture

Physical architecture

Environmental and physical security

Electrical and environmental controls

Human resources security

Availability

Business continuity and disaster recovery

ServiceNow infrastructure operations management

Instance integrations

Authentication and authorization

Security logging and monitoring

Software development: security by design

ServiceNow security operations management

Vulnerability management

Information life cycle and data management

Encryption

Mobile application security

Summary

# Introduction

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

This white paper describes ServiceNow's security program across a number of key security domains. These include architecture, information lifecycle, physical security, security operations, disaster recovery and 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.

While this white paper can serve as a standalone summary of the ServiceNow security program, by design it forms part of the ServiceNow Trust Journey, which leads up to this summary.

## Definitions and context

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 set per customer instance—there is no combining of data or other forms of multi-tenancy.

### ServiceNow cloud

ServiceNow instances operate on a single cloud platform that consists of one user interface, one code base, a common API, and one data model. This is supported by a global support organisation, operating to a single set of processes and tools, under a common governance and compliance structure. 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 obtain the benefits of shared

infrastructure, while taking advantage of the security benefits of customer-specific isolation at the application and data layers. In addition to the security features that come standard within the platform and each instance, customers can access additional security features within their ServiceNow instances.

### 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 can be found at <https://www.servicenow.com/now-platform.html>.

### Instance

An instance is an entirely discrete ServiceNow environment consisting of two or more application nodes and a single database which stores all data, code, and configuration data for the instance. Production instances are automatically replicated to passive data centers, whereas sub-production instances only exist in a single data center.

## 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 as an organization uses

Definitions and context

Information security governance and risk management

Privacy and regulatory compliance

Architecture

Physical architecture

Environmental and physical security

Electrical and environmental controls

Human resources security

Availability

Business continuity and disaster recovery

ServiceNow infrastructure operations management

Instance integrations

Authentication and authorization

Security logging and monitoring

Software development: security by design

ServiceNow security operations management

Vulnerability management

Information life cycle and data management

Encryption

Mobile application security

Summary

this best practice methodology and its principles 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 expressed in its Information Security Management System (ISMS) and its associated security policy 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 in a manner in accordance with overall security policy.

### ServiceNow's SOPs include but are not limited to:

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

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 CEO. This simple organizational structure provides an executive level of visibility and oversight with respect to 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 governance, 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 makes good use of information security best practices in its security processes, e.g. segregation of duties and four-eyes requirements.

## Risk management

ServiceNow has defined processes and procedures for managing and accessing information system and operational security risks. Regular assessments are performed in order 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. Quarterly security and risk oversight meetings are held to discuss the security and risk items that are relevant to the organization by key internal stakeholders.

ServiceNow manages any risks identified as is required, in a timely and effective manner, to safeguard ServiceNow systems and customer data and ensure minimal disruption to its services.

ServiceNow executive leadership is briefed on a regular basis regarding current and new security risks, as well as on potential threats and related matters that could impact ServiceNow and its customers.

## Definitions and context

Information security governance and risk management

Privacy and regulatory compliance

Architecture

Physical architecture

Environmental and physical security

Electrical and environmental controls

Human resources security

Availability

Business continuity and disaster recovery

ServiceNow infrastructure operations management

Instance integrations

Authentication and authorization

Security logging and monitoring

Software development: security by design

ServiceNow security operations management

Vulnerability management

Information life cycle and data management

Encryption

Mobile application security

Summary

## Overall security responsibilities

ServiceNow provides its customers with extensive capabilities to configure their instances to meet their own security policies and requirements. The combination of customer, ServiceNow, and data center responsibilities provides coverage across the entire application and infrastructure stack. The areas of responsibility are shown below.

Responsibility	Area of Responsibility		
	Customer	ServiceNow	Colocation (data center provider)
Data management (classification and retention)	■		
Media disposal and destruction		■	
Backup and restore		■	
Authentication and authorization	■		
Data encryption at rest	■		
Data encryption in flight	■	■	
Encryption key management	■	■	
Security logging and monitoring	■	■	
Vulnerability management	■	■	
Business continuity and disaster recovery		■	
Secure SDLC processes	■	■	
Penetration testing	■	■	
Privacy	■	■	
Compliance: regulatory and legal	■	■	■
Infrastructure management		■	
Security management		■	
Secure configuration of instance	■		
Employee vetting or screening	■	■	■
Environment controls		■	■
Physical security		■	■

Table 1 - Responsibility Map

## Definitions and context

### Information security governance and risk management

### Privacy and regulatory compliance

## Architecture

### Physical architecture

### Environmental and physical security

### Electrical and environmental controls

### Human resources security

### Availability

### Business continuity and disaster recovery

### ServiceNow infrastructure operations management

### Instance integrations

### Authentication and authorization

### Security logging and monitoring

### Software development: security by design

### ServiceNow security operations management

### Vulnerability management

### Information life cycle and data management

### Encryption

### Mobile application security

## Summary

## ServiceNow organizational entitlement reviews

ServiceNow as an organization conducts quarterly entitlement reviews to ensure the appropriate logical and physical rights are assigned to ServiceNow personnel. This includes those responsible for management of its private cloud and physical colocation spaces. Changes to the role of a member of ServiceNow personnel results in the access entitlement being appropriately adjusted without undue delay.

A service catalog of ServiceNow roles and request types is implemented internally. This is used both for new requests and re-assignment 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.

ServiceNow has a dedicated identity and access management (IAM) team with an active IAM entitlement program which requires frequent reassertion of entitlement and comprehensive review.

## Privacy and regulatory compliance

### Privacy

ServiceNow customers are responsible for determining the collection, storage, usage, sharing, archiving, and destruction of data processed in their ServiceNow instances. As the data controller, ServiceNow's customers are responsible for meeting the requirements of relevant privacy legislation in the jurisdictions in which they operate and from which they collect personal data. ServiceNow fulfills the role of the data processor and complies with any obligations this entails. ServiceNow has no visibility or understanding of the conditions under which the data was collected, if appropriate permission was obtained, or whether it is being used in accordance with those conditions.

ServiceNow's primary responsibility with regard to privacy is to protect the confidentiality of any data its customers entrust to it. Regardless of how a customer has

classified the data they choose to store in their instances, ServiceNow implements a single operating and security model for the protection of that data.

Customer data remains the property of that customer at all times. For example, if and when an individual requests information directly from ServiceNow on any data that may be stored about them, or requests to change said data, ServiceNow will always refer that individual to the customer who owns the data.

## Regulatory and industry compliance

ServiceNow has a dedicated governance, risk, and compliance (GRC) team responsible for a number of organizationwide compliance efforts, including managing ServiceNow's compliance program. As part of this, they engage 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. It does, however, have many customers who are, and through the features in the Now Platform and organizational transparency, it is able to support those regulated customers in meeting their obligations.

In addition, ServiceNow operates a quality management system based on the ISO 9001 standard. The ServiceNow QMS has a dedicated QMS team, quality engineering team, and compliance team to ensure continual improvement of its QMS.

ServiceNow has a comprehensive geographical and industry compliance strategy to support customers. This includes:

## Definitions and context

Information security governance and risk management

Privacy and regulatory compliance

Architecture

Physical architecture

Environmental and physical security

Electrical and environmental controls

Human resources security

Availability

Business continuity and disaster recovery

ServiceNow infrastructure operations management

Instance integrations

Authentication and authorization

Security logging and monitoring

Software development: security by design

ServiceNow security operations management

Vulnerability management

Information life cycle and data management

Encryption

Mobile application security

Summary

## ServiceNow certifications/attestations

## Geography

## Industry or vertical

ISO 27001	International	All
ISO 27017:2015	International	All
ISO 27018	International	All
SSAE 18 SOC 1 Type 2	International	All
SOC 2 Type 2	International	All
FedRAMP JAB High and DoD IL 4 authorization	United States	Federal government/DoD
FDA Quality Management System (based on ISO 9001)	International	Life science
US Privacy Shield (EU/US and Switzerland/US)	International	All
ASD Certified Cloud Service	Australia	Australian federal government
Multi-Tier Cloud Security Standard for Singapore (MTCS) Level 3	Singapore	All

Table 2 - ServiceNow Certification/Attestation

## Architecture

ServiceNow's architecture provides the template for the ServiceNow private cloud on which the Now Platform is deployed as a subscription service. The cloud is deployed on a highly standardized, redundant, and managed environment. From pre-built racks through to supporting services, such as networking and other logical infrastructure supporting a defense-in-depth model, ServiceNow's cloud exclusively hosts instances of the Now Platform. Each instance is dedicated to a single customer and accessible only by that customer.

ServiceNow operates its cloud out of colocation data centers which provide robust physical and environmental controls. In these locations, ServiceNow's own on-site personnel exclusively provide management, installation, maintenance, and support.

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, in accordance with 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 only use ServiceNow issued endpoints and a client VPN with two-factor authentication. Access takes place within a virtual sandbox on the endpoint from which employees cannot extract or copy data.



## Definitions and context

### Information security governance and risk management

### Privacy and regulatory compliance

## Architecture

### Physical architecture

### Environmental and physical security

### Electrical and environmental controls

### Human resources security

### Availability

### Business continuity and disaster recovery

### ServiceNow infrastructure operations management

### Instance integrations

### Authentication and authorization

### Security logging and monitoring

### Software development: security by design

### ServiceNow security operations management

### Vulnerability management

### Information life cycle and data management

### Encryption

### Mobile application security

## Summary

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. This approach includes highly restricted networking rule sets regarding ingress and egress requirements and deployment of standardized, hardened systems. These result in a minimal number of necessary services, protocols, and ports being required in provision of the ServiceNow private cloud, thus minimizing attack surfaces.

This exclusive, highly defined and limited environment allows for a number of key benefits:

### Automation

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

### Support, scalability, security

ServiceNow is solely focused on supporting one service: the Now Platform. This is deployed in a private cloud environment dedicated solely to this purpose, and implemented identically in all regions in which ServiceNow operates. The cloud environment supports thousands of identically provisioned 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.

### Control

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

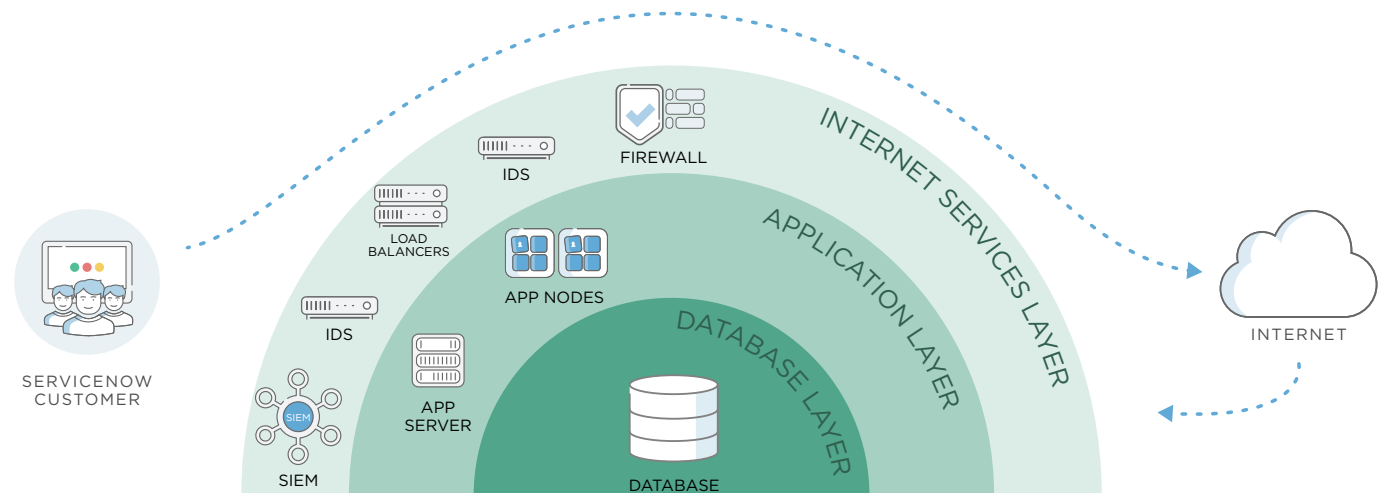


Figure 1 - Three-tier logical architecture model

Definitions and context

Information security  
governance and risk  
management

Privacy and regulatory  
compliance

Architecture

Physical architecture

Environmental and  
physical security

Electrical and  
environmental controls

Human resources security

Availability

Business continuity and  
disaster recovery

ServiceNow infrastructure  
operations management

Instance integrations

Authentication and  
authorization

Security logging and  
monitoring

Software development:  
security by design

ServiceNow security  
operations management

Vulnerability management

Information life cycle and  
data management

Encryption

Mobile application security

Summary

## Logical architecture

The logical architecture of the ServiceNow application is a three-tier model as described below.

### Proxy layer (internet services 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.

This 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 with integrated network firewalls, and intrusion detection systems. All are deployed at a minimum 2N basis to provide redundancy. 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

ServiceNow instances and are the termination point for all

inbound requests made by end-users of those instances. Requests are received by the relevant application nodes and processed by them, including being appropriately 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 databases. There is no comingling of any customer data between instances and databases, nor shared multi-tenant databases with data from multiple customers stored therein. For example, if a customer has four instances of ServiceNow, they will have four entirely separate databases and database services, one unique to each instance. These database services may run on different database servers and there is no assumed relationship.



## Definitions and context

### Information security governance and risk management

### Privacy and regulatory compliance

## Architecture

### Physical architecture

### Environmental and physical security

### Electrical and environmental controls

### Human resources security

### Availability

### Business continuity and disaster recovery

### ServiceNow infrastructure operations management

### Instance integrations

### Authentication and authorization

### Security logging and monitoring

### Software development: security by design

### ServiceNow security operations management

### Vulnerability management

### Information life cycle and data management

### Encryption

### Mobile application security

### Summary

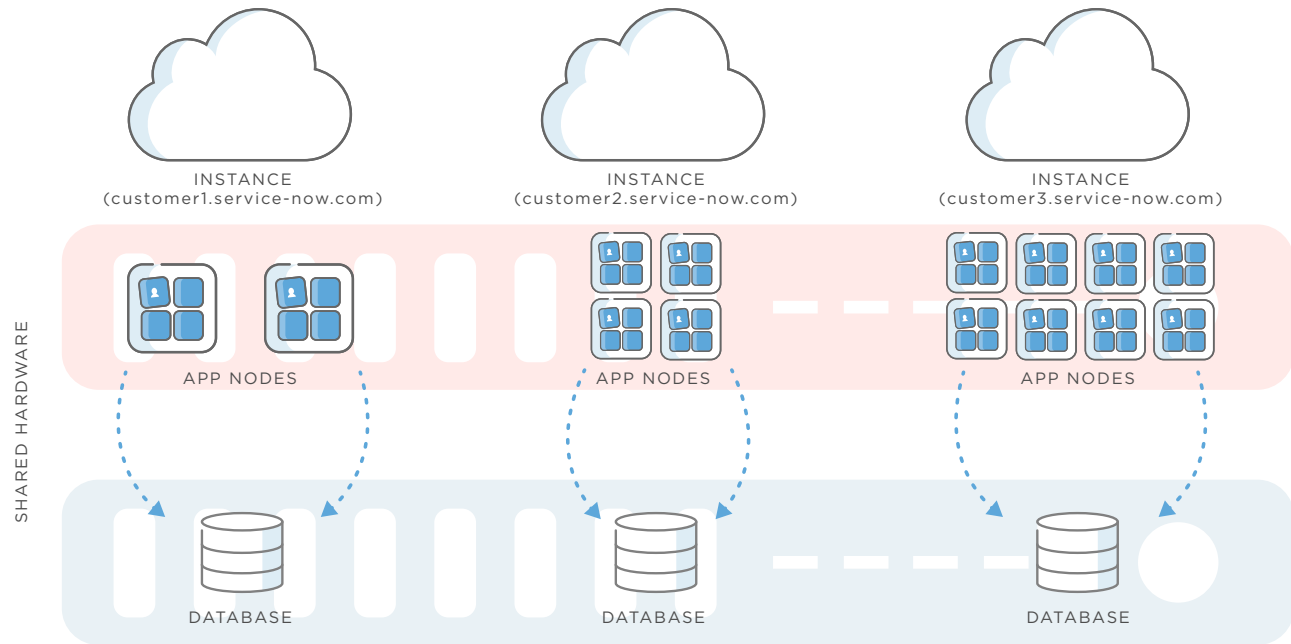


Figure 2: Logically single tenant, physically multi-instance

ServiceNow's customers benefit from multiple layers of robust separation, rather than a single logical control. For example, a number of SaaS provider tenancy models may use tagging of data or records to identify customer data. Access control mechanisms then process these in order to keep customers separated and ensure the data is only visible to the correct customer. Using such techniques has the potential for misalignment of data or records to incorrect owners. Defects, faults, or weaknesses in access control list processing could also potentially lead to data leakage. Because of ServiceNow's defense in depth approach, these two scenarios are extremely unlikely to occur in the ServiceNow multi-instance tenancy model.

A significant benefit of ServiceNow's architecture is that it creates a very distinct boundary between the data of each customer that isn't solely dependent on logical controls. This allows ServiceNow to maintain a highly accurate

inventory of the exact location of a specific customer's data at any given time, and customers can access this information directly via the ServiceNow customer support portal. 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, the fail-over 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. This enables exceptional instance availability.

# Physical architecture

## Geographies

ServiceNow hosts its private cloud in colocation spaces within global data centers arranged in high-availability pairs. Currently ten data center pairs (a total of 20 data centers) exist across four geographic regions. These regions are Asia Pacific Japan (APJ); Europe, Middle East, and Africa (EMEA); North America; and South America.



Figure 3: Data center pairs and support centers

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.

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 maintaining colocation spaces are able to physically access data center locations.

## Physical

ServiceNow's physical architecture supporting its private cloud is deployed into dedicated, ServiceNow-managed colocation spaces and is implemented globally.

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.

## Definitions and context

Information security governance and risk management

Privacy and regulatory compliance

Architecture

Physical architecture

Environmental and physical security

Electrical and environmental controls

Human resources security

Availability

Business continuity and disaster recovery

ServiceNow infrastructure operations management

Instance integrations

Authentication and authorization

Security logging and monitoring

Software development: security by design

ServiceNow security operations management

Vulnerability management

Information life cycle and data management

Encryption

Mobile application security

Summary

## Environmental and physical security

### Overview

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, as described below, are highly secure facilities with 24x7x365 security guards, CCTV, multiple levels of entry controls, and strict procedures for physically entering the facility.

Within each data center all ServiceNow equipment is stored in one or more dedicated anonymous ServiceNow 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.

### Physical data center security

Data centers feature a hardened exterior perimeter with defense-in-depth provided by various access control boundaries.

### 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 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. The detail of the zones will vary between the data centers, but 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, and entrance or exit points are lit. 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 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, secured with access control lists (ACL), and all access is audited.

In addition to CCTV systems, 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 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 or 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 and personnel 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 lock types, including mechanical, biometric readers, and access card readers with PIN entry. 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. Access to the ServiceNow space itself is controlled by ServiceNow using biometric readers, and access card readers with PIN entry. ServiceNow maintains access control lists for its own cages and suites, only permitting limited access for data center personnel where required, i.e. for health and safety purposes.

## Definitions and context

Information security governance and risk management

Privacy and regulatory compliance

Architecture

Physical architecture

Environmental and physical security

Electrical and environmental controls

Human resources security

Availability

Business continuity and disaster recovery

ServiceNow infrastructure operations management

Instance integrations

Authentication and authorization

Security logging and monitoring

Software development: security by design

ServiceNow security operations management

Vulnerability management

Information life cycle and data management

Encryption

Mobile application security

Summary

## 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 interval.

## 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. UPS power is provided either by battery or flywheel systems which can sustain systems until generators can be activated.

## Environmental controls

The heat, ventilation, and air conditioning (HVAC) systems in the data centers are responsible for maintaining 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 set for that zone, alarms will notify 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 between data centers.

Fire detection is provided by very early smoke detection apparatus (VESDA) and heat alarms that are monitored on a 24x7x365 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.

## Human resources security

Upon commencement of the employment process for prospective candidates, ServiceNow undertakes background checks and screening for all roles. 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.

Personnel are also required to undergo annual security and compliance 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

During the term of employment, ServiceNow repeats training on an annual basis, maintains contact with its staff through regular notifications, and provides channels for ServiceNow staff to easily report any suspicious activity.

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, that operate independently

for both the corporate environment and the completely separate customer cloud environment.

Access is role based, in accordance with 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.

## Availability

Availability is an essential element of the ServiceNow security program.

### Overview

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

As ServiceNow's data centers are arranged in pairs, all customer production data is hosted in both data centers simultaneously and kept in sync using asynchronous database replication. Both data centers are active at all times, in a master-master 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 the regional data center pair there is no concept of a fixed primary location for any customer instance. Although requests are not being actively served from both data centers at the same time, they are both "warm" at all times. As there is no data center affinity mechanism, two instances from the same customer could be operating out of different data centers at the same time.

ServiceNow has two distinct processes relating to ensuring instance availability: transfers and failover.

### Transfers

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. ServiceNow commits to with its customers.

## Definitions and context

Information security  
governance and risk  
management

Privacy and regulatory  
compliance

## Architecture

Physical architecture

Environmental and  
physical security

Electrical and  
environmental controls

Human resources security

Availability

Business continuity and  
disaster recovery

ServiceNow infrastructure  
operations management

Instance integrations

Authentication and  
authorization

Security logging and  
monitoring

Software development:  
security by design

ServiceNow security  
operations management

Vulnerability management

Information life cycle and  
data management

Encryption

Mobile application security

Summary

## 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 the former, 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 two-hour recovery time objective (RTO) is targeted by ServiceNow. A maximum one-hour recovery point objective (RPO) is also targeted. Due to the almost real-time replication between data centers, this is usually significantly bested.

Automation technology built on the ServiceNow 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.

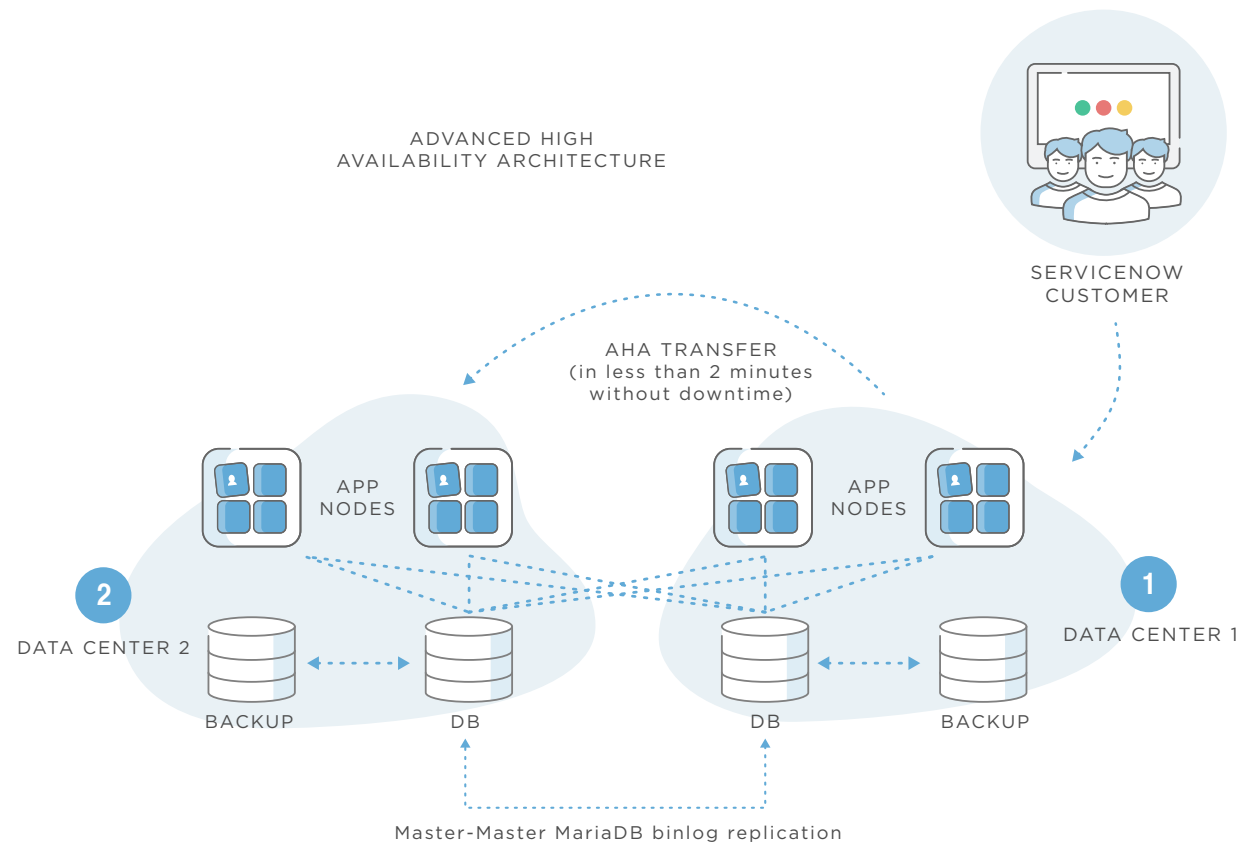


Figure 4: Advanced High Availability Architecture



## Definitions and context

Information security governance and risk management

Privacy and regulatory compliance

Architecture

Physical architecture

Environmental and physical security

Electrical and environmental controls

Human resources security

Availability

Business continuity and disaster recovery

ServiceNow infrastructure operations management

Instance integrations

Authentication and authorization

Security logging and monitoring

Software development: security by design

ServiceNow security operations management

Vulnerability management

Information life cycle and data management

Encryption

Mobile application security

Summary

## Data backup

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. The ServiceNow data backup and recovery system works in parallel to the AHA feature and provides a means to restore previously backed up data.

ServiceNow stores production instance data and their backups in both locations in the customers' elected data center pair. As sub-production instances are not highly available, their data and backups exist only in one location of a data center pair.

The backup cycle consists of four weekly full backups and six daily differential backups which provide 28 days of backups. All backups are written to disk and no tapes or removable media are used. Backups are not sent off-site, but they are made in both data centers within a pair, so benefit from geographic separation. If data is encrypted by the customer in the "live" instance database, then it will also be encrypted in the backups.

ServiceNow restores databases from backups upon a customer's request or in the event of "logical" corruption. This could be, for example, where a customer deletes some data inadvertently. It may also be necessary where a customer's data integration or automation is misconfigured or malfunctions in some way, resulting in data being rendered unusable or inaccessible. In these scenarios, the high availability capability would not assist and hence a restore from backup is the only avenue for recovery. Backups are also used where a system or service failure may in some way impact the integrity of customer data.

Automated testing of backups in progress ensures backup integrity, with any failures reported for remediation within ServiceNow.

The ServiceNow backup architecture is not designed to provide archival records given the maximum 28-day backup retention period; instead it is intended as a recovery process as described previously. 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 within the Now Platform to allow customers to manage logs and regularly export data to external systems as required.

# Business continuity and disaster recovery

## Overview

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 physically and logically isolated from each other. A disaster in 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 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 architecture as previously described in this document.

### 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 BC process covers its corporate environment and functional offices. It is therefore a separate process from that used in its cloud environment. The BC Plan (BCP) has been developed in concert 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.

## ServiceNow infrastructure operations management

As a cloud services provider (CSP), a significant element of ServiceNow's responsibility 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.

## Instance integrations

The Now Platform is based on service-oriented architecture (SOA), in which all data objects can use web services to access bi-directional data-level integration.

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 their 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 ODBC Driver, provided by ServiceNow, and forms, lists, and reports on the platform can be accessed directly using a URL, which facilitates integration on the UI level between two or more web applications.

## Definitions and context

Information security governance and risk management

Privacy and regulatory compliance

## Architecture

Physical architecture

Environmental and physical security

Electrical and environmental controls

Human resources security

Availability

Business continuity and disaster recovery

ServiceNow infrastructure operations management

Instance integrations

Authentication and authorization

Security logging and monitoring

Software development: security by design

ServiceNow security operations management

Vulnerability management

Information life cycle and data management

Encryption

Mobile application security

Summary

## 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 a customer in conjunction with their instances for enterprise application and service monitoring, integration, Orchestration, and Discovery.

The MID Server is a Java application, provided by ServiceNow to customers via a download link within their instance. It may be installed on a host system of the customer's choosing within their environment. The server can be Windows, Unix, or Linux operating system.

By default, a MID server initiates an outbound session every 15 seconds, to a customer's instance over HTTPS, looking for activities to perform. For example, a ServiceNow Discovery activity to update a customer's configuration management database within their instance. The activity is retrieved, executed, and any output returned to the originating instance. This "pull" approach negates the need to open inbound access through a customer's perimeter or firewalls.

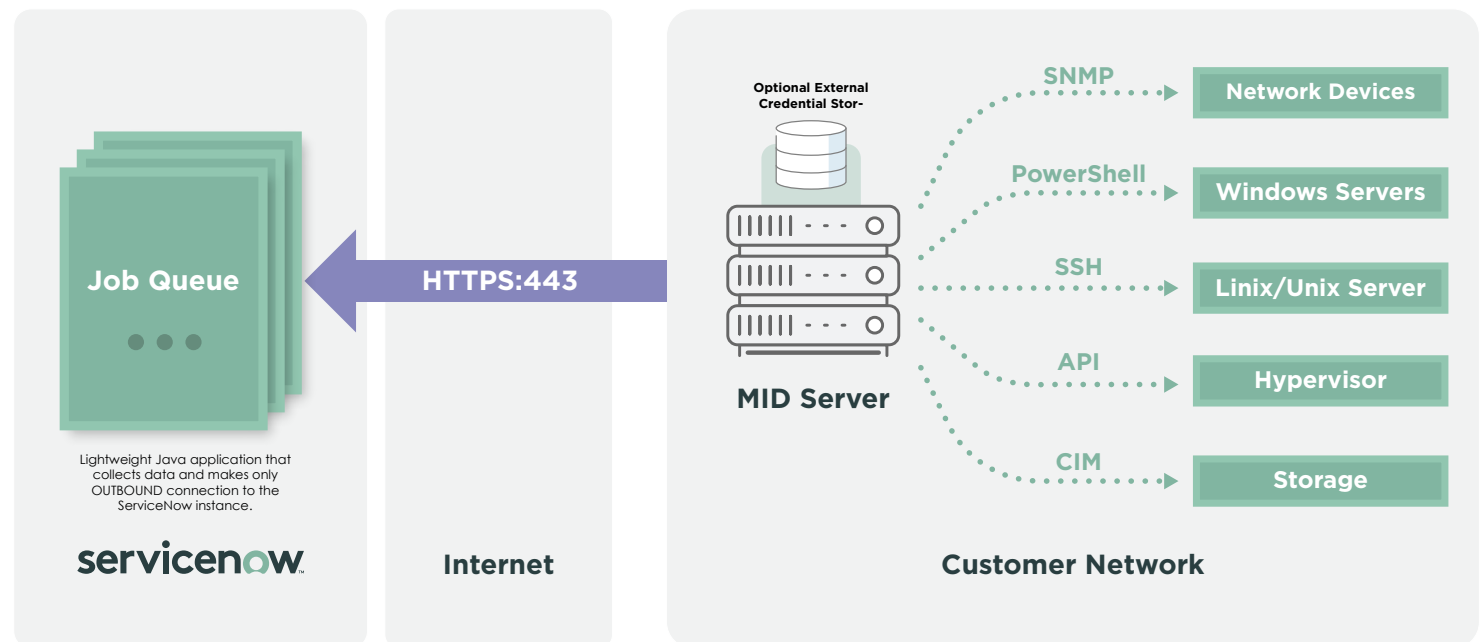


Figure 5: MID Server integration diagram

## Web services

ServiceNow supports Web Services using SOAP and REST for integration and therefore 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.

Support for WS-Security 1.1 in the form of WSS X.509 Token Profile and WSS Username Token Profile is available for incoming SOAP requests. In this context "incoming" means requests targeting a web services resource in a customer ServiceNow instance.

Definitions and context

Information security  
governance and risk  
management

Privacy and regulatory  
compliance

Architecture

Physical architecture

Environmental and  
physical security

Electrical and  
environmental controls

Human resources security

Availability

Business continuity and  
disaster recovery

ServiceNow infrastructure  
operations management

Instance integrations

Authentication and  
authorization

Security logging and  
monitoring

Software development:  
security by design

ServiceNow security  
operations management

Vulnerability management

Information life cycle and  
data management

Encryption

Mobile application security

Summary

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.

## Malware protection

The ServiceNow Antivirus Protection feature protects instances against the uploading or downloading of malicious content. File attachments are scanned by dedicated servers in each regional data center to guard against viruses or malware being distributed from the instance.

## Instance communication hierarchy

Customers initiate communication to their ServiceNow instance over HTTPS, from any endpoint device with a browser or from a system or application level integration. These requests will both originate within the customer's network.

The instance itself never initiates communication into the customer's network unless a data source or other integration to an accessible resource within the customer environment is configured by a customer.

Activities such as ServiceNow Discovery or Orchestration which can "touch" customer infrastructure are executed only on customer direction. These are via activities they define in their instances, using MID Servers they have deployed. Output from the activities, where produced as part of an activity, is sent back to the relevant instance over HTTPS.

A MID Server will only undertake activities and communicate to systems within the customer network as defined by a customer. A customer 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.

# Authentication and authorization

## Authentication

A ServiceNow instance provides a customer with a number of authentication options. All can be used simultaneously within a customer's ServiceNow 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 identity provider (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 (for example, 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 indeed 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 a customer elects to use the SAML plugin, their password and credential policies are governed by their own IdPs.

## Definitions and context

Information security governance and risk management

Privacy and regulatory compliance

Architecture

Physical architecture

Environmental and physical security

Electrical and environmental controls

Human resources security

Availability

Business continuity and disaster recovery

ServiceNow infrastructure operations management

Instance integrations

Authentication and authorization

Security logging and monitoring

Software development: security by design

ServiceNow security operations management

Vulnerability management

Information life cycle and data management

Encryption

Mobile application security

Summary

## Lightweight Directory Access Protocol (LDAP)

LDAP authentication lets customers use their own LDAP-compliant directory services such as Active Directory or similar. A directory needs to be accessible to the relevant ServiceNow instance, as often these are located behind a firewall or other perimeter control.

“Meta” directories including Lightweight Directory Services can alternatively be utilized to permit safe access to a customer’s LDAP directory from a DMZ or similar. Secure LDAP (LDAPS) is supported.

With an LDAP integration, the authentication path commences with an end-user 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. Multiple Directory Service sources may be configured.

As part of the LDAP integration, passwords are not stored nor transferred back to the customer’s ServiceNow instance.

Customers who elect to use their own LDAP directories have their password and credential policies governed by the policies set within these.

### Built-in “native” authentication

In the case of native authentication, passwords as well as other user attributes are managed solely by the customer within their instances of ServiceNow. This is the only authentication method where both the username and password are stored within a customer’s ServiceNow instance.

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

In this authentication option, passwords are stored as a 1-way SHA-256 hash, with an appropriate salt value.

## 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 a customer 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 will 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.

Additionally, and as described previously, integration with a customer’s own directory services is also possible. This then enables a customer to leverage existing users and groups in those directory services to manage users and access within their ServiceNow instances.



## Definitions and context

Information security governance and risk management

Privacy and regulatory compliance

Architecture

Physical architecture

Environmental and physical security

Electrical and environmental controls

Human resources security

Availability

Business continuity and disaster recovery

ServiceNow infrastructure operations management

Instance integrations

Authentication and authorization

Security logging and monitoring

Software development: security by design

ServiceNow security operations management

Vulnerability management

Information life cycle and data management

Encryption

Mobile application security

Summary

## User identity synchronization

A ServiceNow instance requires every user to exist as an identity within its 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. User object passwords cannot be synchronized.

User and group objects can be uploaded into a ServiceNow instance through the use of import sets. These can utilize various types of data source 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 can also be used for ongoing synchronization of these. 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 are not in their ServiceNow instance, SAML user provisioning can automatically create the users in the instance.

A common approach to maintaining identity data is for a customer 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 a customer's 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 a customer to allow their ServiceNow instances through their perimeter and firewall in order to access their internal directory servers. Instead, the customer installs 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 customer's instance. These would then be automatically imported or updated in the target user or group tables within the instance.

## Customer access management

ServiceNow customers are responsible for the management of user identities within their instances. This includes the creation of individual identities 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.

### High Security Settings

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

The plugin enforces 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, as well as other hardening attributes. ServiceNow adds new security properties in each release. Advice and guidance can be found in ServiceNow's Security Best Practice and Instance Hardening guides on ServiceNow Community.

## Security logging and monitoring

For the purposes of customer security, ServiceNow collects and retains logs and events relevant to its entire cloud infrastructure. It also collects information on 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.

Events that occur within a customer instance are accessible to that customer in their instance logs. Events that happen to a customer instance are captured in ServiceNow's infrastructure logs.



## Definitions and context

Information security governance and risk management

Privacy and regulatory compliance

Architecture

Physical architecture

Environmental and physical security

Electrical and environmental controls

Human resources security

Availability

Business continuity and disaster recovery

ServiceNow infrastructure operations management

Instance integrations

Authentication and authorization

Security logging and monitoring

Software development: security by design

ServiceNow security operations management

Vulnerability management

Information life cycle and data management

Encryption

Mobile application security

Summary

## 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 in any way 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 SIEM environment. This can be achieved using the syslog probe, utilizing 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 their specific requirements.

Transaction logs represent every click, view, and system event that occurs in an instance. As a result, they will grow very quickly. These logs include a level of detail useful for customers when troubleshooting issues, as well as providing detailed intelligence on behaviors within an instance.

## ServiceNow infrastructure

A key component of any security program is to maintain detective controls. These are required 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. Its incident response process includes event discovery, triage, escalation, notification (including customer notification), remediation, and post-mortem review. If a customer environment or data is impacted, the customer will be notified via their normal support contacts without undue delay. Contractual commitments can be viewed by accessing the DPA here: <http://www.servicenow.com/schedules.html>

ServiceNow has deployed a redundant intrusion detection system (IDS) monitoring network traffic as it transits into its cloud network. This feeds 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

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.

As well as 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 customer data and customizations within their 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; in other words, it is retained indefinitely in the instance.

## Definitions and context

### Information security governance and risk management

### Privacy and regulatory compliance

## Architecture

### Physical architecture

### Environmental and physical security

### Electrical and environmental controls

### Human resources security

### Availability

### Business continuity and disaster recovery

### ServiceNow infrastructure operations management

### Instance integrations

### Authentication and authorization

### Security logging and monitoring

### Software development: security by design

### ServiceNow security operations management

### Vulnerability management

### Information life cycle and data management

### Encryption

### Mobile application security

### Summary

tasked with network, device, and security events. Alerts and notifications are generated by the SIEM systems in accordance with pre-defined triggers and metrics that are updated constantly. These are reviewed by a 24x7x365 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 used for their 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, with infrastructure events being kept for one year.

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

## Software development: Security by design

### Overview

As a leading SaaS provider, it is essential that security is an integral part of our software development efforts.

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 which 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 covering web application security. This includes, but is not limited to that from organizations such as the Open Web Application Security Project (OWASP).

### Application security testing

ServiceNow's penetration testing regime is a vital component of its development practices and as a result the penetration testing program is wide-ranging and extensive.

### Testing during development

Application security testing occurs throughout the development phase. This is undertaken using a variety of approaches. During development, code for the ServiceNow main branch is subject to continuous ongoing testing and review within ServiceNow using a variety of methods. Commercial and in-house automated toolsets, including static 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.

Dynamic application security testing (DAST) is performed on all currently supported versions of the Now Platform. Appropriate patches and hotfixes are included in the scope of this testing. ServiceNow manages and maintains commercially available and custom toolsets for testing. These are continually reviewed and changes are made as necessary, as the Now Platform evolves.

Any validated security issue found is also checked for and if necessary remediated in all earlier supported versions. 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 comes a phase of external application penetration testing. The intention of this process is to

## Definitions and context

### Information security governance and risk management

### Privacy and regulatory compliance

## Architecture

### Physical architecture

### Environmental and physical security

### Electrical and environmental controls

### Human resources security

### Availability

### Business continuity and disaster recovery

### ServiceNow infrastructure operations management

### Instance integrations

### Authentication and authorization

### Security logging and monitoring

### Software development: security by design

### ServiceNow security operations management

### Vulnerability management

### Information life cycle and data management

### Encryption

### Mobile application security

## Summary

provide 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 which can be shared with existing customers using that version once released.

### Customer application penetration testing

Another significant aspect of ServiceNow's application penetration testing regime is tests performed by its customers.

Through a documented process on the HI customer support portal, existing customers are permitted to

perform an annual application penetration test. 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.

Customers must upgrade their instances to the latest release and patch version prior to any testing taking place. They must also implement ServiceNow's hardening guide before conducting any testing. Testing without these pre-requisites will result in false positive identification of previously identified issues. As a requirement for the process, customers are required to share their 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. Confirmed vulnerabilities discovered by this process are remediated in accordance with 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.

## Application security teams

ServiceNow has dedicated teams of security engineers who are part of the ServiceNow security office and 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

Definitions and context

Information security governance and risk management

Privacy and regulatory compliance

Architecture

Physical architecture

Environmental and physical security

Electrical and environmental controls

Human resources security

Availability

Business continuity and disaster recovery

ServiceNow infrastructure operations management

Instance integrations

Authentication and authorization

Security logging and monitoring

Software development: security by design

ServiceNow security operations management

Vulnerability management

Information life cycle and data management

Encryption

Mobile application security

Summary

# 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.

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

As described previously in this document, ServiceNow has intrusion detection capabilities within its private cloud. In addition, all relevant services and system components send security logs and events to a SIEM for security monitoring and alerting.

## Distributed denial of service (DDoS)

ServiceNow employs a significant range of detective controls to monitor and prevent potential 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 services to mitigate against such attacks.

## Vulnerability management

At a high level, vulnerability management at ServiceNow falls into two primary domains: Now Platform and cloud infrastructure.

### Now Platform

ServiceNow generally 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 you are benefiting from the most current security, performance and functional fixes, ServiceNow will apply patches to your instance(s) 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) to the minimum required patch version.

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

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

## Definitions and context

### Information security governance and risk management

### Privacy and regulatory compliance

## Architecture

### Physical architecture

### Environmental and physical security

### Electrical and environmental controls

### Human resources security

### Availability

### Business continuity and disaster recovery

### ServiceNow infrastructure operations management

### Instance integrations

### Authentication and authorization

### Security logging and monitoring

### Software development: security by design

### ServiceNow security operations management

### Vulnerability management

### Information life cycle and data management

### Encryption

### Mobile application security

## Summary

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.

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 you discover a vulnerability, please report it to us in a responsible manner per the guidelines located [here](#).

Alternate techniques are also used to address vulnerabilities where no clear remediation, i.e. a vendor patch, is available. So-called “virtual” patching is implemented in such circumstances as necessary.

Once it is determined that a patch needs to be deployed, this effort enters the change management process. In 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.

ServiceNow again 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.

## Information lifecycle and data management

### Information classification

ServiceNow applies a single data classification 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 in accordance with its policies for all customer data.

Customers remain the data owner and data controller for all data they place into their ServiceNow instance, and

should apply access controls to restrict access to data within their instances based on their own requirements and needs, in accordance with 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 and the customer’s configuration of their instance(s).

For data deleted by a customer from their instance, the deletion in terms of regular access will take place immediately, and will take 28 days to be cycled out of a backup of that instance.

### Media disposal

ServiceNow hosts its customer data only on solid-state or mechanical disks within its colocation spaces. No tapes or other forms of removable media are used in providing the service, including for backups.

Where functional storage devices are retired due to end-of-life or for re-assignment to new customers, these are logically shredded using a process based on guidance from NIST.

Failed devices are securely stored within the same colocation space where they were formerly used. These are then physically shredded in a destruction process managed and performed by ServiceNow. Storage devices are tracked and recorded throughout this process. The disk destruction process applies to all failed disks whether they were used for customer or any other data.

### 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, if requested, ServiceNow will supply a customer’s data in an SQL dump format. Customers have 45 days to request their data to be returned, after which all hosted backed-up data is automatically deleted and overwritten.



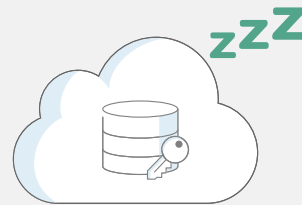
# Encryption

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; a detailed ServiceNow Encryption Technical Summary white paper that describes these features in more detail is also available.

## 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

### Now Platform Encryption

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

## Column encryption

**Fields and attachments:** A built-in feature which provides symmetric data encryption on a per field basis. Customers may select AES128, AES256 or 3-TDEA (3DES) as encryption algorithms and are required to provide suitable encryption keys. Customer keys are re-encrypted (wrapped) with a secondary key to mitigate compromise of customer encrypted data. Data stored in fields encrypted with this feature cannot be searched or reported on. Fields in the instance with a “system” flag or those used in customer workflows and automation cannot be encrypted.

## Edge encryption

**Fields and attachments:** An additional cost feature which performs data encryption inside a customer’s network using encryption keys stored and managed only within that customer’s network. All encryption takes place inside a customer’s network via a proxy application that functions as a cloud access security broker (CASB). When utilizing this feature, unencrypted target data is never stored in a customer’s ServiceNow instance. Edge encryption also includes tokenization and substitution of data that matches standard data structures such as credit card or social security numbers.

**Further information on both of these encryption features is detailed in:**

<https://www.servicenow.com/content/dam/servicenow/documents/whitepapers/wp-data-encryption-with-servicenow.pdf>.



## Definitions and context

## Information security governance and risk management

## Privacy and regulatory compliance

## Architecture

## Physical architecture

## Environmental and physical security

## Electrical and environmental controls

## Human resources security

## Availability

## Business continuity and disaster recovery

## ServiceNow infrastructure operations management

## Instance integrations

## Authentication and authorization

## Security logging and monitoring

## Software development: security by design

## ServiceNow security operations management

## Vulnerability management

## Information life cycle and data management

## Encryption

## Mobile application security

## Summary

## Infrastructure at-rest data encryption

### Database encryption

Database encryption encrypts all customer data at rest in the database with no impact to functionality. It utilizes 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 AES256 encryption. This technology, often called “tablespace encryption” or “transparent data encryption”, is fully transparent to the customer and to the application. ServiceNow applications as well as custom applications can operate seamlessly without any changes necessary because the application always has access to the data it needs in the clear. When using database encryption all data is encrypted, including attachments, logs, and backups.

### Full disk encryption

An additional cost feature which provides encryption for data at-rest only, via self-encrypting hard drives. AES256 bit encryption is implemented in these devices and in the key storage appliances that support them. This capability also requires the purchase of dedicated ServiceNow hardware at further additional cost. It is solely intended to mitigate data exposure through the loss or theft of 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. 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. Customers may also choose to use clear text protocols such as FTP or HTTP if desired.

### 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. This feature is subject to a customer’s email infrastructure being capable of establishing an encrypted handshake with the ServiceNow cloud environment.

### Key management

Encryption keys provided by customers for use with the column encryption feature are backed up within the database for the customer instance where they are used. Customers should back up column encryption keys prior to applying them to their instances.

As previously stated for column encryption, customer keys are re-encrypted using a wrapper key, commonly referred to as a key-encrypting key, which is stored and managed from a key management appliance.

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.

## Definitions and context

## Information security governance and risk management

## Privacy and regulatory compliance

## Architecture

## Physical architecture

## Environmental and physical security

## Electrical and environmental controls

## Human resources security

## Availability

## Business continuity and disaster recovery

## ServiceNow infrastructure operations management

## Instance integrations

## Authentication and authorization

## Security logging and monitoring

## Software development: security by design

## ServiceNow security operations management

## Vulnerability management

## Information life cycle and data management

## Encryption

## Mobile application security

## Summary

Encryption keys used within ServiceNow's cloud infrastructure are managed by ServiceNow. Organizational key management consists of a number of components. 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.

Standard operating procedures are used for the procurement, generation, and configuration of key appliances. Work instructions are used for the configuration and backup of key management appliances with logs from these forwarded to the ServiceNow internal SIEM infrastructure.

## Mobile application 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 previously outlined. Once authenticated, mobile users are subject to the same access controls as other users.

### 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, though that is configurable.

### Application distribution

ServiceNow's mobile applications can be distributed with common Enterprise Mobility Management (EMM) or Mobile Device Management (MDM) platforms.

## Summary

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 and 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, please visit [www.servicenow.com](http://www.servicenow.com) or contact your account representative.