

7 Proven Methods for Strengthening ServiceNow Security

ServiceNow is crucial for managing IT services, business processes, and sensitive data, but its flexibility introduces unique security challenges. Implementing these proven methods will help you secure your environment and mitigate potential vulnerabilities.

1 Regularly Review and Tighten Role-Based Access Controls (RBAC)

ServiceNow's RBAC structure can become complicated, leading to role creep and excessive permissions. Ensure your Access Control Lists (ACLs) are correctly configured and regularly audited to prevent unauthorized access.

Key Actions:

Use **Automated Role Reviews** to detect over-privileged users and streamline permissions.

Implement **Least Privilege** by dynamically adjusting roles to match current responsibilities.



2 Lock Down System Configurations and API Permissions

Misconfigurations in system settings or API permissions are common entry points for attackers, especially when workflows involve sensitive data like CMDB records or IT assets.

Key Actions:

Secure critical settings, such as **API permissions** and **data import/export rules**, to minimize exposure.

Set alerts for unauthorized changes to **business rules** or **workflows**.

3

Enforce Security Baselines for Customizations

ServiceNow's extensive customization capabilities can lead to security risks if not managed properly. Consistent enforcement of security baselines helps protect against misconfigurations.

Key Actions:

Define and Apply Security Baselines: Establish baseline policies for data access, user permissions, and system configurations, and enforce them consistently.

Detect and Correct Policy Deviations: Automatically identify and remediate deviations from established security baselines.



Control External User Access and Activities

External collaborators like partners or vendors often require access to ServiceNow, but this can create data exposure risks. Limit access to only what's necessary and monitor their activities.

Key Actions:

Assign **specific roles** and **restricted permissions** for external users, ensuring they can only access what is strictly necessary.

Continuously monitor external user activity, setting up alerts for suspicious behavior, such as unauthorized data access or changes to configurations.

4

5

Secure Third-Party App Integrations

ServiceNow integrates with third-party apps like Slack and DocuSign to extend functionality. But, these integrations can introduce vulnerabilities if not properly managed, especially through unvetted APIs or excessive permissions.

Key Actions:

Use **OAuth Scopes** to restrict third-party app permissions to only what's necessary.

Regularly **audit and monitor** app configurations and API usage for **unsecured endpoints** or **unusual activity**.





Run Continuous Compliance Audits and Remediate Gaps

Compliance with frameworks like SOC 2 and GDPR are crucial when managing sensitive data within ServiceNow. Automating compliance audits can reduce manual effort and ensure standards are consistently met.

Key Actions:

Schedule **Automated Compliance Scans** against your security policies.

Generate on-demand **Compliance Reports** to demonstrate adherence to regulatory requirements.

6

Detect and Respond to Threats with Advanced Monitoring

Privilege escalations or abnormal data access patterns could indicate a compromised account or insider threat. Implement centralized monitoring to detect and quickly respond to potential threats.

Key Actions:

Centralize Logs for Threat Detection: Aggregate logs from key ServiceNow modules to spot suspicious patterns and potential threats.

Set Alerts for High-Risk Activities: Enable alerts for actions like privilege changes or unusual data access to quickly mitigate security risks.



Secure Your ServiceNow Environment with AppOmni

AppOmni helps you implement these best practices by continuously monitoring permissions, enforcing security baselines, and managing third-party integrations. Our platform automates compliance checks, detects threats early, and integrates security alerts into ServiceNow for faster incident response, keeping your data secure and compliant.

About AppOmni

AppOmni, the leader in SaaS Security, helps customers achieve secure productivity with their applications. Security teams and owners can quickly detect and mitigate threats using unmatched depth of protection, continuous monitoring, and comprehensive visibility. Trusted by over 25% of the Fortune 100, AppOmni specializes in securing diverse SaaS environments.

© 2024 All Rights Reserved

Learn more at appomni.com/critical-apps/service-now-security/