PlatformProtect™
ServiceNow Assessment

Private and Confidential

Note: This is a sample report. Some sensitive data and table rows have been removed and/or anonymised.

Table of Contents

Executive Summary

On February 26, 2025, GetSome conducted a comprehensive assessment of your ServiceNow Development, Test, and Production instances. This assessment evaluated security, data privacy, platform health, and subscription management to identify operational health and risk exposure.

Significant security vulnerabilities and non compliant configurations are present in all instances, including **11 high-severity (P1/P2) issues impacting the Production instance.** These issues represent active risks to platform security and data privacy.

The overall security, privacy and platform health ranking of your ServiceNow environment is **Weak**.

A prioritised set of the issues accompanied by recommended actions your organisation can take to improve security and privacy posture is provided in the Recommendations section. The Remediation section provides a project plan, timeline and cost estimate to remediate the prioritised issues. Immediate focus on high-severity issues is advised. Addressing all recommended items would improve your ranking from a poor **Weak** ranking (score of 65.6%) to a high **Marginal** ranking (score of 90%).

We recommend that you implement a maintenance program that focuses on sustaining improvements achieved through remediation. An example maintenance plan is provided in the Maintenance section.

Current state

PlatformProtect ranking: Weak	**Overall %**	**Dev %**	**Test %**	**Staging %**	**Prod %**
Overall	**65.6**	**60.4**	**63.3**	**63.5**	**75.3**
ServiceNow Instance Hardening Score	86.8	86.0	86.0	87	88
Instance Hardening	69.9	68.8	68.8	72.3	69.7
Security	73.1	71.0	72.9	69.0	79.7
Security Best Practice	20.3	0.6	22.3	27.3	31.1
Security Metrics	49.8	14.6	54.7	63.8	66.3
Data Privacy	55.4	51.2	51.2	59.5	59.5
Platform Health	43.3	27.7	44.2	50.4	51.1
Subscription Management	53.3				53.3

*The ServiceNow Instance Hardening score is a proprietary ServiceNow score. ServiceNow recommends a score over 90% as a minimum acceptable score.

Note:

1. PlatformProtect scores are calculated upon the percentage of compliant items weighted against higher priority non compliant items.
2. Overall score is an average of all other PlatformProtect scores.
3. Ranking: **Weak** - score less than 86%, **Marginal** - score between 86% and 91%. **Good** - score between 91% and 93%, **Strong** - score above 93%

Assessment Methodology

Automated and manual checks assessed the Security and Platform Health of each ServiceNow instance, with separate checks for Privacy and Subscription Management. The Security Center and Instance Scan applications were updated, adding over 300 additional checks across Security, Manageability, Upgradability, Performance, and User Experience. Over 50 Security Best Practices and 80 Security Metrics were also reviewed.

In total, over 600 checks and 160+ best practices/metrics were evaluated per instance. Findings were consolidated into recommended actions, with PlatformProtect Scores calculated for Instance Hardening, Security, Data Privacy, Platform Health, and Subscription Management.

This report provides a summary of findings with detailed finding information available within each ServiceNow instance.

Legend: Finding Note	Non compliant or violates best practice
	Current state acceptable but can improve
	Current state compliant

Actions Undertaken

The following actions were carried out in each instance as part of the assessment.

Security	**Priority**	**Description**	**Finding Note**	**Best Practice**
Current State				
Review: **Security Center Version**	P2 - High	Determine if the latest version of Security Center is installed	Version 1.3.1 (out of date)	Cell contents removed for sample report
Document: **Current Instance Hardening Score**	P4 - Low		Prod: 86, Test: 86, Dev: 84, Rating WEAK	…
Document: **Current Security Center Version**	P4 - Low		Version 1.3.1 (out of date)	…
Document: **Last Instance Hardening Scan date**	P4 - Low		17 September 2023 (out of date)	…
Update Security Center and Hardening Scan	**Priority**	**Description**	**Finding Note**	**Best Practice**
Update: **Security Center**	P2 - High	Update Security Center to latest version	Updated to Version 1.5 (current)	Cell contents removed for sample report
Execute: **Instance Hardening Scan**	P2 - High	Obtain new hardening Score with latest version of Security Center	Executed: 26th Feb 2025	…
Document: **Instance Hardening Score**	P4 - Low	Document items requiring review with client	Prod: 86, Test: 86, Dev: 84, Rating WEAK	…
Review: **Non-compliant Hardening Scan Items**	P3 - Moderate	Form part of the starting set of items to address	34 found: Recommend to remediate 23	…

Document: **Non-compliant Hardening Scan Items**	P3 - Moderate	Document items requiring review with client	34 found: P1 - 1, P2 - 8, P3 - 18, P4 12	…
Manual checks	**Priority**	**Description**	**Finding Note**	**Best Practice**
Execute: **Manual Security Checks**	P2 - High	A set of additional security checks performed outside of Security Center	Executed: 26th Feb 2025	Cell contents removed for sample report
Document: **Manual Security Checks**	P3 - Moderate	Required to set new baseline for Security Posture	4 additional P2 items detected	…
Review: **Security Best Practice Items (Xanadu ->)**	P3 - Moderate	Xanadu onwards: Best Practice items are indicated and should be reviewed and actioned	No best practice items completed in instances	…
Document: **Security Best Practice Items (Xanadu ->)**	P3 - Moderate	Document items requiring review with client	11 identified for review with client	…
Review: **Security Metrics**	P3 - Moderate	Over 80 metrics provide insight to weakness and improvement items	Metrics not being reviewed. Multiple metrics tagged for review due to risk associated with not reviewing	…
Document: **Security Metrics**	P3 - Moderate	Document items requiring review with client	8 identified for review with client	…
Review: **Critical Updates** (Customer Actions)	P3 - Moderate	Customer Actions need to be assessed and addressed	2 Critical Updates exist - 1 overdue	…
Document: **Critical Updates** (Customer Actions)	P3 - Moderate	Customer Actions need to be assessed and addressed	3DES Password2, MFA	…
2 ROWS REMOVED FROM SAMPLE REPORT				
Privacy	**Priority**	**Description**	**Finding Note**	**Best Practice**
Data Privacy App				
Review: Data Privacy Setup	P2 - High	Determine if Data Privacy application has been configured	Application not available	Cell contents removed for sample report
Review: Zero Trust check	P2 - High	Yokohama - determine if Zero Trust policies in place for PII	Zero Trust policies not established	…
Manual Checks	**Priority**	**Description**	**Finding Note**	**Best Practice**
Review: User (sys_user) PII fields	P1 - Critical	Identify User PII fields	No additional PII fields added to User table	Cell contents removed for sample report
Review: User PII fields - additional protection	P2 - High	Determine if additional privacy protection exists on User PII fields	No additional protection in place for PII fields	…
14 ROWS REMOVED FROM SAMPLE REPORT				
Platform Health & Best Practice	**Priority**	**Description**	**Finding Note**	**Best Practice**
Current State				

Review: **Instance Scan Application**	P2 - High	Used to understand current instance health	Completed: 26th Feb 2025	Cell contents removed for sample report
Document: **Current Instance Scan Count**	P4 - Low		84 checks - 2103 occurrences	…
Document: **Last Instance Scan Date**	P4 - Low		14 September 2024 (out of date)	…
Instance Scan	**Priority**	**Description**	**Finding Note**	**Best Practice**
Import: **Additional Checks x 5**	P2 - High	Required to set new baseline for Security Posture	Completed: 26th Feb 2025	Cell contents removed for sample report
Execute: **Full Instance Scan**	P2 - High	Required to set new baseline for Platform Health	Executed: 26th Feb 2025	…
Review: **Non compliant Instance Scan Items**	P3 - Moderate	Required to set new baseline for Platform Health	84 checks - 2297 occurances	…
Document: **Non compliant Instance Scan Items**	P4 - Low	Document items requiring review with client	Completed: 26th Feb 2025	…
Manual checks	**Priority**	**Description**	**Finding Note**	**Best Practice**
Execute: **Manual Platform checks**	P2 - High	Multiple manual checks	Completed: 26th Feb 2025	Cell contents removed for sample report
Document: **Manual Platform Checks**	P3 - Moderate	Document items requiring review with client	Completed: 26th Feb 2025	…
8 ROWS REMOVED FROM SAMPLE REPORT				
Subscriptions & Licensing	**Priority**	**Description**	**Finding Note**	**Best Practice**
Current State				
Review: **Subscription Dashboard**	P2 - High	Done to understand current licensing posture	Completed: 26th Feb 2025	Cell contents removed for sample report
Document: **Subscription overage - Users**	P3 - Moderate	Identify User over-subscription	Overage on 2 of 8 subscriptions	…
Document: **Subscription overage - Custom Tables**	P3 - Moderate	Identify Table over-subscription	No overage of Table Subscription	…
Review: **Groups linked to Dashboard**	P2 - High	Identify if Groups are being linked to Subscription Dashboard	Multiple Groups not linked to Subscription Dashboard	…
Review: **Custom Tables linked to Dashboard**	P2 - High	Identify if Tables are being linked to Subscription Dashboard	Custom Tables linked	…
Document: **Current State checks**	P3 - Moderate	Document items requiring review with client	Completed: 26th Feb 2025	…
2 ROWS REMOVED FROM SAMPLE REPORT				

Results

Results revealed 281 open risks identified across the areas of Instance Hardening, Security, Data Privacy, Platform Health and Subscription Management, yielding a **PlatformProtect score* of 65.6%**

Key findings highlight **significant security vulnerabilities** across all instances, including **11 high-severity (P1/P2) issues** and **17 medium-severity (P3) issues directly affecting the Production instance**. These gaps pose potential operational, compliance, and cost inefficiencies if unaddressed.

The overall Security Privacy and Platform Health ranking of your ServiceNow environment is **Weak**.

PlatformProtect ranking: Weak	Overall %	Dev %	Test %	Staging %	Prod %
Overall	**65.6**	**60.4**	**63.3**	**63.5**	**75.3**
ServiceNow Instance Hardening Score	86.8	86.0	86.0	87	88
Instance Hardening	69.9	68.8	68.8	72.3	69.7
Security	73.1	71.0	72.9	69.0	79.7
Security Best Practice	20.3	0.6	22.3	27.3	31.1
Security Metrics	49.8	14.6	54.7	63.8	66.3
Data Privacy	55.4	51.2	51.2	59.5	59.5
Platform Health	43.3	27.7	44.2	50.4	51.1
Subscription Management	53.3				53.3

*The ServiceNow Instance Hardening score is a proprietary ServiceNow score. ServiceNow recommends a score over 90% as a minimum acceptable score.

Note:

4. PlatformProtect scores are calculated upon the percentage of compliant items weighted against higher priority non compliant items.
5. Overall score is an average of all other PlatformProtect scores.
6. Ranking: **Weak** - score less than 86%, **Marginal** - score between 86% and 91%. **Good** - score between 91% and 93%, **Strong** - score above 93%

Instance Hardening

Ensuring that instance hardening controls are implemented is vital to reducing the risk of attack to your ServiceNow environment. The Instance Hardening score of 69.9% (PlatformProtect) and 83% (ServiceNow) indicates that minimal effort has been… **DETAILS REMOVED FROM SAMPLE REPORT**

Instance Hardening: Weak	Overall	Dev %	Test %	Staging %	Prod %
ServiceNow Instance Hardening Score	**87.0**	**87.0**	**87.0**	**87.0**	**87.0**
PlatformProtect Score	**69.9**	**68.8**	**68.8**	**72.3**	**69.7**
Total checks assessed	880	220	220	220	220
Total non compliant	119	31	31	28	29
Severity: Critical	0	0	0	0	0
High	31	8	8	7	8

Medium	52	14	14	12	12
Low	36	9	9	9	9
Total occurrences	1035	278	280	232	245

Security

The Security checks addressed here do impact overall security but are not considered part of the Instance Hardening checks. The poor score achieved for Security is due in part to a large number of customisations performed by two individual developers… **DETAILS REMOVED FROM SAMPLE REPORT**

Security: Weak	**Overall**	**Dev %**	**Test %**	**Staging %**	**Prod %**
PlatformProtect Score	**73.1**	**71.0**	**72.9**	**69.0**	**79.7**
Total checks assessed	224	56	56	56	56
Total non compliant checks	41	11	10	11	9
Priority 1- Critical	3	1	1	1	0
2 - High	9	2	2	3	2
3 - Moderate	14	5	3	3	3
4 - Low	15	3	4	4	4
Total occurrences	7558	2014	1894	1760	1890

Critical updates (Customer Actions)

ServiceNow Critical Updates are ones that need to be reviewed and addressed as they will have an impact upon the operation of your ServiceNow environment. Of the three Critical Updates present in your environment one has been addressed in Prod… **DETAILS REMOVED FROM SAMPLE REPORT**

Critical Updates: Weak	**Overall**	**Dev %**	**Test %**	**Staging %**	**Prod %**
PlatformProtect Score	**22.6**	**15.8**	**15.8**	**15.8**	**42.9**
Total checks assessed	16	4	4	4	4
Total non compliant checks	11	3	3	3	2
Priority 1- Critical	4	1	1	1	1
2 - High	7	2	2	2	1
Total occurrences	11	3	3	3	2

Security Best Practice

The Security Best Practice Items provide a foundation for good security governance and where appropriate should be adopted. With confirmation that very few of the best practices have previously been reviewed or put into practice the score for this… **DETAILS REMOVED FROM SAMPLE REPORT**

Best Practice: Weak	Overall	Dev %	Test %	Staging %	Prod %
PlatformProtect Score	**20.3**	**0.6**	**22.3**	**27.3**	**31.1**
Total checks assessed	2344	586	586	586	586
Total non compliant checks	291	80	73	68	70
Priority 1- Critical	10	4	2	2	2
2 - High	103	31	26	24	22
3 - Moderate	108	27	27	26	28
4 - Low	70	18	18	16	18

Security Metrics

The Security metrics extant within a ServiceNow instance provide a view of the security landscape that should not be ignored. WIth the confirmation that security metrics are not being reviewed and the recorded exports from the User (sys_user) table reported there… **DETAILS REMOVED FROM SAMPLE REPORT**

Security Metrics: Weak	Overall	Dev %	Test %	Staging %	Prod %
PlatformProtect Score	**49.8**	**14.6**	**54.7**	**63.8**	**66.3**
Total checks assessed	324	81	81	81	81
Total non compliant checks	108	46	24	20	18
Priority 1- Critical	4	1	1	1	1
2 - High	22	11	5	3	3
3 - Moderate	44	22	8	8	6
4 - Low	38	12	10	8	8

Data Privacy

The low Data Privacy score is a concern, given the nature of data held within the ServiceNow environment. No significant attempt to consider or protect data privacy is visible in the environment and this combined with recorde instances of data export from the User… **DETAILS REMOVED FROM SAMPLE REPORT**

Data Privacy: Weak	Overall	Dev %	Test %	Staging %	Prod %
PlatformProtect Score	**55.4**	**51.2**	**51.2**	**59.5**	**59.5**
Total checks assessed	48	12	12	12	12
Total non compliant checks	18	5	5	4	4
Priority 1- Critical	4	1	1	1	1
2 - High	4	1	1	1	1
3 - Moderate	6	2	2	1	1
4 - Low	4	1	1	1	1
Total occurrences	32	10	10	6	6

Platform Health

The Platform Health score encompasses checks for Security, Performance, Manageability, Upgradability and User Experience. High priority non compliant items were detected in all areas.The largest contributor to the low Platform Health score is the significant customisation… **DETAILS REMOVED FROM SAMPLE REPORT**

Platform Health: Weak	Overall	Dev %	Test %	Staging %	Prod %
PlatformProtect Score	**43.3**	**27.7**	**44.2**	**50.4**	**51.1**
Total checks assessed	1316	329	329	329	329
Total non compliant checks	260	78	64	60	58
Priority 1- Critical	20	7	5	4	4
2 - High	21	6	5	5	5
3 - Moderate	138	41	33	33	31
4 - Low	81	24	21	18	18
Total occurrences	5524	2106	1328	1045	1045

Subscriptions and Licensing

The recent contact from ServiceNow regarding overage of both SPM and ITSM licenses is a direct indicator that Subscription Management is not being well managed. Opportunities do however exist to easily improve this area and begin to optimise licensing spend… **DETAILS REMOVED FROM SAMPLE REPORT**

Subscription Management: Weak	Overall				Prod %
PlatformProtect Score	**53.3**				**53.3**
Total checks assessed	8				8
Total non compliant checks	3				3
Priority 1- Critical	1				1
2 - High	2				2
3 - Moderate	0				0
4 - Low	0				0
Total occurrences	3				3

Recommendations

Guided by a desire to improve the security, data privacy, platform health and licensing posture of your ServiceNow environment, it is recommended that a remediation program be undertaken to address the most pressing issues identified. Remediation needs to occur across all instances of ServiceNow.

From experience, remediating security issues can be complex and we suggest a pragmatic approach which aims to improve security posture rapidly by initially remediating a mix of high-priority items and high-value low-complexity items.

This approach allows for not only high-priority issues to be addressed but also allows for many of the quick-win items of less complexity to be remediated helping to improve the overall security posture of your environment.

Total estimated time to remediate all recommended items is 11 days. Remediation of all recommended items would improve instance scores and PlatformProtect ranking as shown below.

Estimated ranking post full remediation

PlatformProtect ranking: Marginal	**Overall %**	**Dev %**	**Test %**	**Staging %**	**Prod %**
Overall	**90.0**	**89.1**	**89.6**	**90.3**	**91.0**
ServiceNow Instance Hardening Score	90.7	90.6	89.7	90.7	91.7
Instance Hardening	91.8	89.8	89.8	93.8	93.7
Security	88.1	87.0	88.9	85.0	91.7
Security Best Practice	90.5	90.6	90.9	90.3	90.1
Security Metrics	90.1	88.6	88.7	91.8	91.3
Data Privacy	90.4	90.2	90.2	90.5	90.5
Platform Health	88.6	88.7	89.2	90.4	86.1
Subscription Management	93.3				93.3

Current pre-remediation ranking

PlatformProtect ranking: Weak	**Overall %**	**Dev %**	**Test %**	**Staging %**	**Prod %**
Overall	**65.6**	**60.4**	**63.3**	**63.5**	**75.3**
ServiceNow Instance Hardening Score	86	86	86	87	88
Instance Hardening	69.9	68.8	68.8	72.3	69.7
Security	73.1	71.0	72.9	69.0	79.7
Security Best Practice	20.3	0.6	22.3	27.3	31.1
Security Metrics	49.8	14.6	54.7	63.8	66.3
Data Privacy	55.4	51.2	51.2	59.5	59.5
Platform Health	43.3	27.7	44.2	50.4	51.1
Subscription Management	53.3				53.3

Instance Hardening

Recommended for remediation

The following items have been recommended for remediation due to their high priority nature and impact upon hardening score.

<table>
<tr><th>Priority
-
Severity</th><th>Hardening check</th><th>Hardening Score Impact*</th><th>PlatformProtect Score Impact*</th><th>Remediation Complexity</th><th>Remediation Estimate **</th></tr>
<tr><td><b>P2 - 8.2</b></td><td><b>Enable SNC Access Control Plugin</b></td><td>+0.66</td><td>+0.5</td><td>Basic</td><td>1 hour</td></tr>
<tr><td colspan="6"><b>Security risk</b>: Unnecessary exposure of instance access to a wider group of people.
<b>Finding details</b>: This weakness exists in all instances.</td></tr>
<tr><td><b>P2 - 7.2</b></td><td><b>Activate Role Based Multi-Factor Authentication</b></td><td>+0.56</td><td>+0.5</td><td>Moderate</td><td>4 hours</td></tr>
<tr><td colspan="6"><b>Security risk</b>: If this property is not enabled, there is a risk of unauthorized access to sensitive data.
<b>Finding details</b>: This has been partially done for users holding the Admin role, however MFA is now required best practice for all users that are not using SSO to login. This applies to all instances of ServiceNow.</td></tr>
<tr><td><b>P2 - 8.1</b></td><td><b>Enable Email Spam Scoring and Filtering</b></td><td>+0.63</td><td>+0.5</td><td>Basic</td><td>1 hour</td></tr>
<tr><td colspan="6"><b>Security risk</b>: Email filters enable administrators to use a condition builder or conditional script to specify when to ignore malicious incoming emails from known/unknown sender. Email is never filtered, blocked, or quarantined from the instance as part of spam scoring. It is only scored and then sent on to the instance. All filtering is done within the instance with the Email Filters plugin.
<b>Finding details</b>: This applies primarily to the Production and Staging instances as email receiving is disabled in the Development and Test instances.</td></tr>
<tr><td colspan="6"><b>15 rows removed from sample report</b></td></tr>
</table>

*Remediation of all recommended items would improve the ServiceNow Instance Hardening Score by 5.1, lifting the ServiceNow Hardening score from 86 to 91, while lifting the PlatformProtect Score from to 86.8 (Rating: **Marginal**) to 93.8 (Rating: **Strong**)

**Estimate covers remediation in all instances.

Recommended client actions

Place a priority upon hardening of the ServiceNow environment. Implement a maintenance schedule and allocate budget to address identified non compliant hardening activities. If not already started, then suggest a program of work be undertaken to remediate the… **DETAILS REMOVED FROM SAMPLE REPORT**

Security

Recommended for remediation

The following items have been recommended due to their high priority nature, impact upon hardening score and remediation complexity.

<table>
<tr><th>Priority - Area</th><th>Instance Scan check</th><th>PlatformProtect Score Impact*</th><th>Remediation Complexity</th><th>Remediation Estimate **</th></tr>
<tr><td><b>P1 - Security</b></td><td><b>Triple DES Usages in Password2 Fields</b></td><td>+1.0</td><td>Moderate</td><td>1 - 2 hours</td></tr>
<tr><td colspan="5"><b>Security risk</b>: 1: Security Weakness: 3DES is outdated and vulnerable to attacks (e.g., brute-force, meet-in-the-middle) due to its smaller key size and weaker design compared to AES. This increases the risk of unauthorized decryption of sensitive password2 data (e.g., API keys, credentials).

2: Non-Compliance: Failure to deprecate 3DES violates NIST standards (e.g., NIST SP 800-131A), which disallow 3DES for secure encryption post-2023. This could lead to audit failures or regulatory penalties.

3: Data Exposure: Existing 3DES-encrypted password2 data remains at risk until updated. If exploited, attackers could access sensitive integration credentials or other secrets stored in these fields.

<b>Finding details</b>: Occurrences of Password2 fields that are using 3DES encryption are identified in all instances.</td></tr>
<tr><td><b>P2 - Security</b></td><td><b>Check for invalid roles, groups and inheritance</b></td><td>+0.5</td><td>Moderate</td><td>1 - 2 hours</td></tr>
<tr><td colspan="5"><b>Security risk</b>: 1: Unauthorized Access: Invalid or misconfigured roles and group memberships (e.g., roles not properly inherited or orphaned roles) could grant users unintended access to sensitive data or functionality, violating the principle of least privilege.

2: Security Breaches: Without verifying role and group integrity, attackers could exploit inconsistencies (e.g., roles lingering after group removal) to escalate privileges or access restricted areas.

3: Compliance Violations: Failure to ensure proper role inheritance and group assignments may lead to non-compliance with security standards (e.g., NIST, ISO 27001), risking audit failures or penalties.

4: Operational Disruptions: Incorrect role assignments could disrupt workflows, as users might lack necessary permissions or have excessive access, causing inefficiencies or errors.

<b>Finding details</b>: Multiple occurrences located in all instances.</td></tr>
<tr><td><b>P2 - Security</b></td><td><b>Longer session time out may cause performance issues</b></td><td>+0.5</td><td>Basic</td><td>0.5 hour</td></tr>
<tr><td colspan="5"><b>Security risk</b>: User sessions being active for an indefinite amount of time is a security risk and should expire on a time-based configuration. Do not set this value to more than one day.

<b>Finding details</b>: Current timeout in Production and Staging exceed the best practice value.</td></tr>
<tr><td><b>P2 - Security</b></td><td><b>Do not use ‘gr’ as a variable name</b></td><td>+0.5</td><td>Moderate</td><td>2 - 4 hours</td></tr>
<tr><td colspan="5"><b>Security risk</b>: Using gr as a GlideRecord variable name in global scripts poses the following risks:</td></tr>
</table>

1: Variable Collision: Since ServiceNow’s JavaScript runs in a global scope, a gr variable defined in one script (e.g., a business rule) can overwrite another gr in a different script within the same transaction. This clobbers the original object, leading to unpredictable behavior. 2:Data Corruption: Your script might update or query the wrong record—or even a different table—because the overwritten gr now references an unrelated object. For example, a script meant to update an incident could accidentally modify a user record. 3:Logic Errors: Subsequent lines of code will execute assuming gr is the intended GlideRecord, potentially returning no results (if reassigned to an empty query) or incorrect results, disrupting business processes. 4: Security Implications: If sensitive data (e.g., user permissions, PII) is involved, unintended updates or queries could expose or alter it, breaching security controls. **Finding details**: Multiple occurrences exist in all instances.
25 rows removed from sample report

*Remediation of all recommended items would improve the PlatformProtect Hardening score by 7.0 from 87.0 (Rating: **Marginal**) to 94.0 (Rating: **Strong**).
**Estimate covers remediation in all instances.

Recommended client actions

Immediate steps should be taken to address the number of high priority items identified. A significant improvement in the security posture of the entire ServiceNow environment could be achieved with the targeted remediation of the top twelve identified items. **DETAILS REMOVED FROM SAMPLE REPORT**

Critical Updates (Customer Actions)

Recommended for remediation
The items listed below must be addressed promptly due to their time-sensitive impact. ServiceNow will discontinue support or use of these features in the future, and failing to prepare could result in operational errors or disruptions.

<table>
<tr><th>Priority</th><th>Critical Update</th><th>PlatformProtect Score Impact*</th><th>Remediation Complexity</th><th>Remediation Estimate **</th></tr>
<tr><td><b>P1 - Critical</b></td><td><b>Enable 3DES deprecation for Password2 Fields</b></td><td>+1.0</td><td>Moderate</td><td>4 - 8 hours</td></tr>
<tr><td colspan="5"><b>Security risk</b>: User sessions being active for an indefinite amount of time is a security risk and should expire on a time-based configuration. Do not set this value to more than one day.

<b>Finding details</b>: Current timeout in Production and Staging exceed the best practice value.</td></tr>
<tr><td><b>P1 - Critical</b></td><td><b>MFA Enforcement for all user performing Local or LDAP authentication</b></td><td>+1.0</td><td>Moderate</td><td>2 - 4 hours</td></tr>
<tr><td colspan="5"><b>Security risk</b>: User sessions being active for an indefinite amount of time is a security risk and should expire on a time-based configuration. Do not set this value to more than one day.

<b>Finding details</b>: Current timeout in Production and Staging exceed the best practice value.</td></tr>
<tr><td><b>P1 - Critical</b></td><td><b>End of Support: GlideEncrypter API</b></td><td>+1.0</td><td>Moderate</td><td>4 - 6 hours</td></tr>
<tr><td colspan="5"><b>Security risk</b>: 1: Security Vulnerabilities:
The GlideEncrypter API uses 3DES, which NIST 800-131A Rev 2 deems insecure due to its susceptibility to attacks (e.g., brute-force, meet-in-the-middle). Post-December 2023, continued use for encryption leaves data (e.g., in password2 fields) exposed to potential breaches.

2: Compliance Violations:
NIST guidelines retired 3DES for encryption after December 2023, allowing only legacy decryption. Retaining GlideEncrypter past this deadline violates NIST standards, risking audit failures, regulatory penalties, or loss of certifications (e.g., ISO 27001).

3: Operational Disruptions:
Once ServiceNow removes GlideEncrypter in a future release (post-deprecation), scripts or applications relying on it will fail. This could disrupt workflows, integrations (e.g., API key handling), or data access, leading to errors or downtime.

4: Data Integrity Issues:
Without transitioning to AES (the supported standard), encrypted data may become unreadable or incompatible when the API is unsupported, especially if transferred between instances without updated key management (e.g., KMF Key Exchange).

5: Increased Remediation Costs:
Delaying action until removal forces urgent, reactive fixes under pressure, potentially raising costs and complexity compared to proactive migration now.

<b>Finding details</b>: Multiple instances of the use of the GlideEncrypter API was detected in custom code in each instance.</td></tr>
</table>

*Remediation of all recommended items would improve the PlatformProtect Score from to 86.3 to 95.2 (Rating: **Strong**)
**Estimate covers remediation in all instances.

Recommended client actions

Critical actions should be prioritised for review and remediation. Addressing these items before they become impacting to the instance will avoid possible disruption to service or exposure to avoidable vulnerabilities.

Security Best Practice

ServiceNow specifies over 50 Security Best Practice items. These have been reviewed for each instance with recommended remediation items presented below.

Recommended for Review/Action

<table>
<tr><th>Priority</th><th>Best Practice</th><th>PlatformProtect Score Impact*</th><th>Remediation Complexity</th><th>Remediation Estimate **</th></tr>
<tr><td><b>P1 - Critical</b></td><td><b>Change the default login credentials</b></td><td>+1.0</td><td>Basic</td><td>0.5 hours</td></tr>
<tr><td colspan="5"><b>Security risk</b>: 1:Unauthorized Access:
Default passwords, even if unique to the instance, are often predictable or documented. Attackers familiar with ServiceNow can exploit these to gain access, especially to high-privilege accounts like "admin," compromising the entire instance.

2: Privilege Escalation:
The "admin" account has broad control (e.g., modifying ACLs, scripts, or configurations). If unchanged, an attacker could escalate privileges, alter security settings, or access sensitive data (e.g., PII in password2 fields), bypassing intended controls.

3: Operational Disruption:
Accounts like "ITIL" (used for ITSM processes) or "employee" (potentially tied to workflows) with default passwords could be hijacked, leading to unauthorized changes in tickets, workflows, or data—disrupting business operations (e.g., incident management).

4: Data Breach:
Unchanged passwords increase the risk of data exposure. For example, an attacker accessing the "admin" account could extract or manipulate sensitive records, violating privacy (e.g., GDPR) or triggering compliance failures.

5: Brute-Force Vulnerability:
Default passwords are prime targets for brute-force or password-spray attacks. Without changes, these accounts lack the complexity to resist such attempts, especially if not paired with MFA.

6: Audit and Compliance Failures:
Retaining default credentials violates security best practices (e.g., NIST 800-63B) and ServiceNow's guidance. This could fail audits, incur penalties, or weaken trust in the instance's security posture.

<b>Finding details</b>: Default User accounts exist in all instances without password change.</td></tr>
<tr><td><b>Action</b></td><td colspan="4">Review each default account and force a password change.</td></tr>
</table>

P2 - High	**Disable browser SQL messages**	+0.5	Basic	0.5 hours
Security risk: 1: Exposure of Sensitive Information: If glide.db.loguser is not set to false, server-side error messages—including stack traces and database structure details—may be shown to end-users. This exposes internal system information that should remain hidden. 2: Increased SQL Injection Vulnerability: These error messages can reveal database schema, table names, or query details. An attacker could exploit this knowledge to craft targeted SQL injection attacks, especially if other vulnerabilities (e.g., poor input validation) exist, potentially compromising data integrity or confidentiality. 3: Weakened Defense-in-Depth: Displaying error messages to users undermines a key security layer. Even without immediate vulnerabilities, this leakage reduces the instance's resilience by giving attackers reconnaissance data, making future exploits easier. 4: Operational and Reputational Impact: If exploited, this could lead to unauthorized data access, service disruptions, or breaches, damaging trust and incurring compliance penalties (e.g., GDPR, HIPAA) if sensitive data is exposed. **Finding details**: This issue is detected only in the Development instance, however, as the Development instance is accessible without IP Address restriction any attacker can reach this instance and attempt to exploit this vulnerability.				
Action	Disable the display of SQL error messages in the Development instance. If this is a requirement for testing then ensure a process where it is disabled after testing is completed.			
P1 - Critical	**Disable password-less authentication**	+1.0	Basic	4 hours
Security risk: An attacker is able to log in to the instance with the default usernames, or by specific individual/group (usually firstname.lastname) without any password. Doing so is viewed as a critical security risk, because it would enable a public user to violate the confidentiality and integrity of the instance data. **Finding details**: This is an **extremely dangerous** setting to have detected as being non compliant. It appears only in the Test instance and should be **remediated immediately**. This setting appears to have been altered on the 11th November 2024.				
Action	The "**Disable password-less authentication**" setting in the Test instance should be **remediated immediately**.			
22 rows removed from sample report				

*Remediation of all recommended items would improve the PlatformProtect Security Score to 89.5 (from 83.0). Minimum acceptable target score is 91.0
**Estimate covers remediation in all instances.

Recommended client actions

Immediate steps should be taken to address the number of high priority items identified. A significant improvement in the security posture of the entire ServiceNow environment could be achieved with the targeted remediation of the identified items.

Security Metrics

ServiceNow specifies over 80 Security Metrics. Many of these indicate where a possible vulnerability may lay. The metrics should be monitored routinely for threshold changes that indicate a Security (or Privacy(breach. Each of the metrics has been reviewed for each instance with recommended remediation items presented below.

Recommended for Review/Action

<table>
<tr><th>Priority</th><th>Security Metric</th><th>PlatformProtect Score Impact*</th><th>Remediation Complexity</th><th>Remediation Estimate **</th></tr>
<tr><td><b>P2 - High</b></td><td><b>Number of Users using MFA Bypass</b></td><td>+0.5</td><td>Basic</td><td>1 hour</td></tr>
<tr><td colspan="5"><b>Security risk</b>: 1: Weakened Authentication Security:
Impact: MFA adds a critical layer of protection beyond passwords. Bypassing it for many users—especially if not limited to service accounts—reverts authentication to single-factor (e.g., username/password), making it easier for attackers to gain access if credentials are compromised (e.g., via phishing).

Context: The ServiceNow Security Best Practices Guide (Page 12) emphasizes MFA as a key defense. Widespread bypass undermines this.

2: Increased Vulnerability to IP Spoofing or Network Breaches:
Impact: If attackers spoof a trusted IP (e.g., via VPN manipulation) or breach the company network (e.g., via malware), they can log in without MFA, bypassing the second factor entirely. With many users on bypass, the attack surface grows significantly.

3: Privilege Escalation Exposure:
Impact: If admin or high-privilege users are among those bypassing MFA, a compromised account could grant attackers broad access to configure the instance, access sensitive data, or disrupt operations (e.g., altering workflows).

4: Operational Disruptions from Misconfiguration:
Impact: Managing bypass for a large user base increases the chance of errors (e.g., overly broad IP ranges or missing updates to trusted IPs). This could allow unauthorized access or, conversely, lock out legitimate users, causing downtime or confusion.

5: Compliance Violations:
Impact: Regulations (e.g., GDPR, HIPAA) and security standards (e.g., NIST 800-63) often mandate MFA for sensitive systems. Widespread bypass could lead to non-compliance, risking audits, fines, or reputational damage.

6: Reduced Detection of Anomalous Logins:
Impact: MFA prompts provide a checkpoint to flag unusual activity (e.g., logins from new devices). Bypassing it for many users limits this visibility, delaying detection of brute-force attacks or credential stuffing.

7: Data Exposure Risk:
Impact: ServiceNow instances often store sensitive data (e.g., PII, business records). A high number of bypass users heightens the risk of data breaches if accounts are compromised, especially without MFA's extra verification.

<b>Finding details</b>: This metric shows an unusually high number of users bypassing MFA (27) in the Production instance.</td></tr>
<tr><td><b>Action</b></td><td colspan="4">Review the list of Users currently bypassing MFA in the Production instance and determine if this is warranted. If not then enforce MFA over those users.</td></tr>
</table>

19 rows removed from sample report

*Remediation of all recommended items would improve the PlatformProtect Security Metric Score to 89.5 (from 83.0). Minimum acceptable target score is 91.0
**Estimate covers remediation in all instances.

Recommended client actions

Immediate steps should be taken to review and action the identified Security Metrics. **DETAILS REMOVED FROM SAMPLE REPORT**

Data Privacy

Data Privacy is a growing concern for organisations that store not only Personally Identifiable Information (PII), such as Name, Email, Phone, Gender and Address, but other business sensitive data within their applications.

Recommended for remediation

<table>
<tr><th>Priority</th><th>Data Privacy check</th><th>PlatformProtect Score Impact*</th><th>Remediation Complexity</th><th>Remediation Estimate **</th></tr>
<tr><td><b>P1 - Critical</b></td><td><b>Avoid Public Reports</b></td><td>+1.0</td><td>Basic</td><td>4 hours</td></tr>
<tr><td colspan="5"><b>Privacy Risk</b>: 1: Unauthorized Data Exposure:
Description: When a report is "published" in ServiceNow, it becomes accessible via a public URL (e.g., https://<instance>.service-now.com/sys_report_display.do?sysparm_report_id=<SYS_ID>), requiring no authentication. Anyone with the link—or who can find it through scraping or guessing—can view the data, regardless of whether they have a ServiceNow account.

Impact: Sensitive data (e.g., incident details, user PII, financial metrics) could be exposed to external parties, breaching confidentiality. The community post confirms this: “Publishing a report will make that report available to the entire internet. No authentication required.”

Context: The ServiceNow Best Practices Guide emphasizes controlling access to data, but Public Reports bypass Access Control Lists (ACLs) for visibility, undermining this.

2: Bypass of Security Controls (Including MFA):
Description: Multi-Factor Authentication (MFA) protects instance logins, but Public Reports don’t require login at all. This creates an MFA bypass vector—attackers don’t need credentials or additional factors to access report data.

Impact: Even if your instance enforces MFA for all users, public report links render that irrelevant, exposing data to anyone who obtains the URL. The community discussion doesn’t mention MFA explicitly but underscores the lack of authentication as a core issue.

Context: This contradicts the best practice push for layered security (e.g., MFA, IP restrictions), leaving a gaping hole.

3: Data Leakage Beyond Intended Audience:
Description: Reports meant for internal use (e.g., shared with “Everyone” in the instance) might include sensitive fields (e.g., sys_user names, incident descriptions). Publishing them publicly removes the boundary of instance-level access.</td></tr>
</table>

Impact: Competitors, malicious actors, or unintended insiders could access operational insights, PII, or proprietary info. The community post notes the counterintuitive nature: “very unintuitive that a ‘published’ report would provide that kind of access.”

Context: The Shared Responsibility Model assigns customers responsibility for data management—public exposure shifts blame squarely to misconfiguration.

4: Operational Disruption from Misuse:
Description: Public Reports reflect real-time data (refreshed on access). If widely shared, excessive traffic from external viewers could strain instance performance, especially if reports query large datasets.

Impact: Slowdowns or outages could disrupt workflows.

Context: While not a direct security breach, this ties to the broader health of the instance.

5: Compliance Violations:
Description: Exposing data publicly risks violating regulations like GDPR, HIPAA, or internal policies requiring data protection (e.g., encryption at rest).

Impact: Fines, legal action, or reputational damage could result. Certifications (e.g., ISO 27001), which assume controlled access—Public Reports break that assumption.

6: Difficulty Tracking Access:
Description: Unlike instance logins tracked via logs, Public Report access isn’t logged within ServiceNow, as no authentication occurs.

Impact: You can’t monitor who’s viewing the data or detect misuse.

Finding details: Multiple occurrences of Public Reports exist in all instances.

P1 - Critical	**Exclude PII tables from Clones**	+1.0	Basic	1 hour

Privacy Risk: 1: Unauthorized Access to Sensitive PII:
Description: Sub-production instances (e.g., dev, test, or sandbox environments) often have broader access permissions for developers, testers, or third-party vendors. If the sys_user table—containing PII like names, emails, phone numbers, or even encrypted passwords—is cloned without alteration, unauthorized users could access this data.

Impact: This increases the likelihood of internal misuse or accidental exposure, especially since sub-prod environments lack the strict role-based access controls (RBAC) or multi-factor authentication (MFA) typical in production.

2: Data Breach Exposure:
Description: Sub-production instances are frequently less hardened—lacking firewalls, intrusion detection, or regular security patching—making them prime targets for external attackers. A cloned sys_user table with unmasked PII (e.g., full names, SSNs if stored) could be exfiltrated if the instance is compromised.

Impact: A breach could lead to identity theft, financial fraud, or legal liability, especially if PII falls under regulations like GDPR, HIPAA, or CCPA.

3: Compliance Violations:
Description: Cloning sensitive PII to a less-secure environment without anonymization or encryption violates data protection laws. For example, GDPR mandates minimizing PII exposure, and HIPAA requires strict PHI safeguards—neither of which sub-prod typically meets fully.

Impact: Non-compliance could result in hefty fines, legal action, or reputational damage. ServiceNow’s Shared Responsibility Model places PII protection on the customer, amplifying this risk.

4: Data Leakage via Development or Testing:
Description: Developers or testers might extract data from sub-prod for debugging (e.g., exporting logs or running scripts) or inadvertently expose it via unsecured integrations. If sys_user data retains real PII, this could leak outside the instance—e.g., through misconfigured APIs or email notifications.

Impact: Leaked PII could end up on the dark web or with competitors, eroding trust and triggering mandatory breach notifications.

5: Inability to Detect or Trace Breaches:
Description: Sub-production instances often lack robust logging, monitoring, or audit trails compared to production. If PII from sys_user is accessed improperly, it might go unnoticed without tools like SIEM integration or SSC monitoring (as recommended in the Security Best Practices Guide).

Impact: Delayed detection prolongs exposure, complicating remediation and increasing damage.

6: Operational Disruption from Remediation:
Description: If PII is exposed in sub-prod, retroactive cleanup (e.g., wiping instances, notifying affected users) disrupts development cycles. Preserving sys_user relationships for testing becomes harder if data is scrambled post-clone, defeating the clone’s purpose.

Impact: This creates a trade-off: either risk PII exposure or lose functional parity between prod and sub-prod, slowing development.

7: Reverse Identification Risk:
Description: Even if PII is partially obscured (e.g., scrambling names like “Chuck Tomasi” to “xD8ff3 992x”), clever users could cross-reference related tables (e.g., cmdb_ci for assets or incident for caller info) to re-identify individuals. Sub-prod’s lax security amplifies this risk.

Impact: Partial anonymization isn’t foolproof, leaving residual PII vulnerable to determined insiders or attackers.

Finding details: The Production clone exclusions table does not exclude the User (sys_user) table from cloning. This data is cloned into all three sub-production instances increasing the risk of exposure.

4 rows removed from sample report

*Remediation of all recommended items would improve the PlatformProtect Privacy Score to 89.5 (from 83.0). Minimum acceptable target score is 91.0
**Estimate covers remediation in all instances.

Recommended client actions

A focus should be placed upon the Data Privacy hardening of your ServiceNow environment. As national and global privacy regulations continue to tighten, Data Privacy is becoming a vital area that requires constant attention.

Platform Health Items

Platform Health items are assessed via the Instance Scan application within ServiceNow. The Instance scan executes checks that cover Platform Health areas: Security, Manageability, Upgradability, Performance and User Experience.

Recommended for remediation

<table>
<tr><th>Priority - Area</th><th>Platform Health check</th><th>PlatformProtect Score Impact*</th><th>Remediation Complexity</th><th>Remediation Estimate **</th></tr>
<tr><td>**P1 - Security**</td><td>**Inactive users not locked out**</td><td>+1.0</td><td>Basic</td><td>2 hours</td></tr>
<tr><td colspan="5">**Security risk:** If deactivated users in a ServiceNow instance are not also explicitly locked out, several security risks emerge due to incomplete access revocation:
1: Unauthorized API Access:
Deactivated users retain the ability to authenticate and interact with the ServiceNow environment via the Table API (e.g., REST or SOAP APIs) if their credentials remain valid. For example, a script or integration using their API token could still query or modify sensitive data, such as incident records or user profiles, bypassing the deactivation intent.

2: Data Exposure:
Without a lockout, deactivated users could exploit API access to extract confidential information (e.g., PII, company data) from tables they were previously authorized to view. This undermines data privacy and compliance with standards like GDPR or HIPAA.

3: Malicious Actions:
A deactivated but unlocked account—especially if compromised (e.g., stolen credentials)—could be used to perform unauthorized actions, such as updating records, deleting data, or triggering workflows. For instance, an ex-employee with lingering access could disrupt operations or escalate privileges via API calls.

4: Authentication Loophole:
Deactivation alone doesn't invalidate session tokens or credentials unless lockout is enforced. If a user's session remains active or they re-authenticate via API, they could bypass the deactivation status, contradicting the ServiceNow Security Best Practices Guide emphasis on robust access control (e.g., Page 12).

5: Audit and Compliance Failures:
Failure to fully disable access violates the principle of least privilege and could lead to audit findings. Regulators or internal policies might flag this as a gap, risking penalties or reputational damage, especially if tied to sensitive data exposure.

Finding note: Inactive but not locked out users were detected in all instances.</td></tr>
<tr><td>**P1 - Security**</td><td>**Avoid the eval function**</td><td>+1.0</td><td>Basic</td><td>2 - 4 hours</td></tr>
<tr><td colspan="5">**Security risk:** The eval() function in JavaScript, commonly available in ServiceNow's server-side scripting (e.g., Business Rules, Script Includes), executes a string as code. While powerful, its improper use introduces significant security and operational risks:
1: Injection Attacks:
Risk: If eval() processes untrusted or user-supplied input (e.g., from a form field or API), attackers can inject malicious code. For example, eval("gs.getUser().setPassword('hacked')") could be executed, compromising user accounts or system integrity.

Impact: Unauthorized access, data breaches, or privilege escalation within the ServiceNow instance.

2: Difficulty in Debugging:
Risk: Errors in eval()-executed code lack line numbers or clear stack traces, as the code is dynamically generated rather than part of the original script. For instance, an error like "undefined variable" won't pinpoint the source, slowing down issue resolution.

Impact: Prolonged vulnerabilities or misconfigurations, as admins struggle to identify and fix security flaws.</td></tr>
</table>

3: Unintended Execution:
Risk: Hardcoded or poorly sanitized strings passed to eval() might execute unexpected logic. For example, eval("deleteRecord()") could unintentionally delete critical records if the string's origin isn't controlled.

Impact: Data loss or operational disruptions, undermining platform reliability.

4: Performance Overhead:
Risk: eval() is slower than native code execution, as it requires runtime parsing. In a ServiceNow environment with frequent script execution (e.g., workflows), this can degrade performance.

Impact: Sluggish instance response, potentially exposing timing-based attack vectors.

5: Compliance Violations:
Risk: Using eval() with unsanitized input violates secure coding standards (e.g., OWASP guidelines, ServiceNow's Secure Coding Guide, Page 19 of the Best Practices Guide). This could flag the instance in audits.

Impact: Regulatory penalties or failed security certifications.

Finding note: Only two instances of the use of the eval() function in custom code were detected in each instance.

45 rows removed from sample report

*Remediation of all recommended items would improve the PlatformProtect Platform Health Score to 89.5 (from 83.0). Minimum acceptable target score is 91.0
**Estimate covers remediation in all instances.

Recommended client actions

Immediate steps should be taken to address the number of high priority items identified. A significant improvement in the Platform Health posture of the entire ServiceNow environment could be achieved with the targeted remediation of the identified items. **DETAILS REMOVED FROM SAMPLE REPORT**

Subscriptions and Licensing

Avoiding subscription overage is a responsibility of the ServiceNow Platform Owner. In order to manage subscription allocation correctly both an understanding of license allocation and the Subscription Management Dashboard is required.

Recommended for Remediation

<table>
<tr><th>Priority</th><th>Subscription and Licensing check</th><th>PlatformProtect Score Impact*</th><th>Remediation Complexity</th><th>Remediation Estimate **</th></tr>
<tr><td><b>P1 - Critical</b></td><td><b>Roles directly assigned to Users</b></td><td>+1.0</td><td>Moderate</td><td>4 - 8 hours</td></tr>
<tr><td colspan="5"><b>Licensing risk:</b> 1: Inaccurate License Allocation:
Risk: Without proper setup, the dashboard may fail to accurately track and display license assignments for users. This could lead to over-allocation (using more licenses than purchased) or under-allocation (leaving licenses unused), both of which disrupt compliance and cost efficiency.

Why: The dashboard relies on correct configuration of the subscription data (e.g., Groups linked to the Subscription Management Dashboard).

2: Compliance Violations:</td></tr>
</table>

Risk: Incorrect setup increases the chance of breaching ServiceNow license agreements, potentially triggering audits or penalties from ServiceNow. For example, exceeding licensed user counts or using unentitled features could flag non-compliance. Why: The dashboard provides visibility into compliance status (e.g., via the Subscription Overview widget), but if not configured with accurate subscription records or synced with the latest entitlement data, it won't alert you to violations. 3: Financial Overruns: Risk: You might incur unexpected costs from over-provisioning licenses or failing to reclaim unused ones, inflating your ServiceNow investment without realizing it until billing reconciliation. Why: Proper setup ensures the dashboard tracks license consumption metrics. Errors in setup—like missing role assignments or unlinked subscriptions—hide these insights, delaying cost optimization. 4: Operational Inefficiency: Risk: Admins may struggle to manage user access or deallocate licenses efficiently, leading to delays in provisioning new users or retiring old ones, which could disrupt workflows. Why: The dashboard's tools depend on correct Group and Custom Table linking. Without them, manual tracking becomes necessary, prone to human error and time waste. 5: Audit Preparedness Failure: Risk: Inability to produce reliable license usage reports during an audit could complicate proving compliance, risking disputes with ServiceNow or third-party auditors. Why: The dashboard generates audit-ready data when correctly set up. **Finding note**: Multiple Users were detected to have directly assigned roles. Directly assigned roles are not counted by the Subscription Management Dashboard and can lead to undercounting of license use, leaving you vulnerable to overage charges from ServiceNow. This only applies to the Production instance.				
P1 - Critical	**Link Groups to Subscription Dashboard**	+1.0	Basic	0.5 hours
Licensing risk: As above. **Finding note**: Groups containing assigned roles are not linked to the Subscription Management Dashboard. This will provide an undercount of license usage. This only applies to the Production instance.				
3 rows removed from sample report				

*Remediation of all recommended items would improve the PlatformProtect Subscription and Licensing Score to 89.5 (from 83.0). Minimum acceptable target score is 91.0
**Estimate covers remediation in all instances.

Recommended client actions
Immediate steps should be taken to resolve the Subscription issues detected which will result in ana accurate understanding of the license usage within your ServiceNow environment.

Muted Findings

Not all findings are relevant or pose a risk and some can be muted. Muting a finding leaves the finding in the system but excludes it from reporting, making it easier to identify and manage more important issues.

The following are a list of some findings that we recommend muting as part of a remediation plan. No findings were muted as part of this assessment.

Priority	Check	Reasoning	Item
P2 - High	Public Reports to be verified	This finding relates to a report no longer used on the platform.	Report: Certification Instances
P2 - High	Set glide.invalid_query.returns_no_rows to true	This finding points to an empty record	empty
31 rows removed from sample report			

Recommended client actions

As part of a remediation plan appropriate findings should be muted to make future assessments and analysis easier to perform.

Remediation

Should you wish to commence remediation of the recommended items, GetSome has a remediation plan ready to commence. An estimate of 11 days effort is given to remediate the recommended items.

Coordination with your ServiceNow, Change Management and Cyber teams will be required and their involvement is detailed in the remediation plan.

Detailed remediation documentation, including: Remediation Steps for each item, Test documentation, Change documentation, as Built Documentation and OCM comms (for ServiceDesk, Admins, Developers and other impacted parties) is provided should you choose to remediate with GetSome.

Our goal is to help you reduce risk and improve your ServiceNow.

Remediation Estimate

Estimate of $xx,xxx.00 NZD + GST for 11 days effort.

Remediation Plan

Below is a draft remediation plan estimated at 1 day setup and 10 days remediation.
Rows highlighted in blue indicate activities to be performed by your team.

Resource Titles
PC: Primary Contact (Client)
GS: GetSome Consultant
ADM: ServiceNow Admin (Client)
SC: Cyber/Security Contact (Client)
CM: Change Manager (Client)
PO: ServiceNow Platform Owner (Client)
SD: Service Desk (Client)

Phase - Setup - Duration 1 days		
Entry Criteria		
Signed Contract or PCR for 10 days of remediation		
PC confirmation that Client is ready to remediate		
Inputs		
Assessment Report, Recommended remediation items, Draft Remediation Plan		
Task	**Resources (Responsible)**	
General	**Client**	**GetSome**
Schedule Kickoff meeting	PC	GS
Schedule Closeout meeting	PC	GS
Confirm access to support.servicenow for access to KBs		GS
Change preparation		

Draft - Low Risk Change	PC, CM	GS
Draft - n x additional Changes (based upon remediation plan)	PC, CM	GS
Exit Criteria		
Confirmation from GS that Setup Phase items have completed		GS
Confirmation from PC that Client is ready to begin	PC	GS
Outputs		
Drafted Changes, Kickoff and Closeout meetings scheduled		
Phase - Remediate - Duration 10 days		
Entry Criteria		
Setup Phase complete		
Confirmation from PC that Client is ready to begin		
Inputs		
Assessment Report, Recommended remediation items, Draft Changes, Draft Remediation Plan		
Task	**Resources (Responsible)**	
Kick off meeting: DD/MMM - 1 hour duration	**Client**	**GetSome**
Facilitate Kick-off meeting	PC, SC, ADM, SD, PO, CM	GS
Review the Remediation items	PC, SC, ADM, SD, PO, CM	GS
Identify UAT testers	PC**	GS
Remediate Development Instance	**Client**	**GetSome**
Develop common fixes (Update sets, data files and process steps)		GS
Develop unique fixes (done on point basis)		GS
GetSome testing		GS
UAT Development Instance	**Client**	**GetSome**
Request UAT where appropriate	PC	GS
Perform UAT	PC**	GS
Obtain signoff on UAT	PC	GS
UAT Defect remediation	PC**	GS
Documentation	**Client**	**GetSome**
Update As Built documentation		GS
Approve As Built documentation	PC	
Update Baseline	**Client**	**GetSome**
Rescan environment - Hardening, Additional Security, Full Instance		GS
Update Baseline 1		GS
Remediate Test Instance	**Client**	**GetSome**

Develop common fixes (Update sets, data files and process steps)		GS
Develop unique fixes (done on point basis)		GS
GetSome testing		GS
UAT Test Instance	**Client**	**GetSome**
Request UAT where appropriate	PC	GS
Perform UAT	PC**	GS
Obtain signoff on UAT	PC	GS
UAT Defect remediation	PC**	GS
Documentation	**Client**	**GetSome**
Update As Built documentation		GS
Approve As Built documentation	PC	
Update Baseline	**Client**	**GetSome**
Rescan environment - Hardening, Additional Security, Full Instance		GS
Update Baseline 1		GS
Remediate Staging Instance	**Client**	**GetSome**
Develop common fixes (Update sets, data files and process steps)		GS
Develop unique fixes (done on point basis)		GS
GetSome testing		GS
UAT Staging Instance	**Client**	**GetSome**
Request UAT where appropriate	PC	GS
Perform UAT	PC**	GS
Obtain signoff on UAT	PC	GS
UAT Defect remediation	PC**	GS
Documentation	**Client**	**GetSome**
Update As Built documentation		GS
Approve As Built documentation	PC	
Update Baseline	**Client**	**GetSome**
Rescan environment - Hardening, Additional Security, Full Instance		GS
Update Baseline 1		GS
Remediate Production Instance	**Client**	**GetSome**
Develop unique fixes (done on point basis)		GS
Deploy common fixes (Low Risk Change)		GS
Deploy common fixes (n x Additional Changes)		GS
GetSome testing		GS
UAT Production Instance	**Client**	**GetSome**
Request UAT where appropriate	PC	GS
Perform UAT	PC**	GS
Obtain signoff on UAT	PC	GS
UAT Defect remediation	PC**	GS

Documentation	**Client**	**GetSome**
Update As Built documentation		GS
Approve As Built documentation	PC	
Update Baseline	**Client**	**GetSome**
Rescan environment - Hardening, Additional Security, Full Instance		GS
Update Baseline 1		GS
Closeout meeting	**Client**	**GetSome**
Facilitate Closeout meeting		GS
Review Baseline 0 and 1 and Report with client	PC, PO, ADM	GS
Confirm Remediation Phase Items Complete		GS
Decide upon maintenance approach	PC	GS
Exit Criteria		
Confirmation from GS that Remediation Phase items have completed		GS
Maintenance approach understood	PC	
Project Change Request document signed by both parties (required for Recurring Services)	PC	GS
Outputs		
Baseline 1, Decision on Maintenance (recurring services) approach, As Built documentation, Project Change Request document (optional)		

** Primary Contact responsible for providing UAT signoff

Sample: Change document
Sample: Test document
Sample: OCM document
Sample: As Built document

Maintenance

We recommend that you maintain the improvements gained through remediation by adopting a maintenance plan that focuses on Platform Security, Privacy, Health and Subscription Management.

The following is a sample GetSome PlatformProtect Monthly Maintenance schedule with 1 day assessment and 2 days remediation per month.

The PlatformProtect Maintenance service provides you with ongoing assessment, remediation, updates to Security Center and Instance Scan, plus alerting of Security, Privacy, Platform Health and Subscription events.

Estimate for this plan is $x,xxx.00 + GST per month.

Maintenance Plan

Phase - Setup - Duration 1 day (one time setup)		
Entry Criteria		
Signed agreement to perform PlatformProtect Maintenance		
PC confirmation that Client is ready to commence		
Inputs		
Baseline1 and Assessment Report, As Built documentation		
Task	**Resources (Responsible)**	
General	**Client**	**GetSome**
Schedule Kickoff meeting (Month 1 only)	PC	GS
Schedule Monthly review meeting	PC	GS
Confirm access to support.servicenow for access to KBs		GS
Supply PC with MaintenancePack documentation for review		
Change preparation	**Client**	**GetSome**
Schedule Change for Prod to install PlatformProtect Maintenance Pack		
Setup tasks	**Client**	**GetSome**
Install PlatformProtect Maintenance Pack - Development		
Install PlatformProtect Maintenance Pack - Test		
Install PlatformProtect Maintenance Pack - Production (under Change)		
Setup Clone Exclusions for Platform Protect Pack Prod (under change)		
Exit Criteria		
Confirmation from GS that Setup Phase items have completed		GS
Confirmation from PC that Client is ready to begin maintenance	PC	GS
Outputs		

Drafted Changes, Kickoff and Monthly meetings scheduled		
Phase - Assess - Duration 1 day (monthly)		
Entry Criteria		
Setup Phase Complete		
Confirmation from PC that Client is ready to begin		
Inputs		
Client contact details - Change Manager, Platform Owner, Cyber contact, SNAD		
Task	**Resources (Responsible)**	
Change Preparation	**Client**	**GetSome**
Draft Monthly Change for end of month - Production	PC, CM	GS
Draft Monthly Change for Security Center Update	PC, CM	GS
Draft - Low Risk Change	PC, CM	GS
Draft - n x additional Changes (based upon monthly remediation plan)	PC, CM	GS
Current State	**Client**	**GetSome**
Document current state of Client Environment		GS
Assess: Development Instance	**Client**	**GetSome**
Update **Security Center Application**		GS
Execute **Instance Hardening** scan		GS
Execute **Additional Security Checks** scan checks		GS
Execute **Full Instance Scan**		GS
Perform **Manual checks**		GS
Review and document **Delta Instance Hardening** non-compliant items		GS
Review and document **Delta Additional Security** non-compliant items		GS
Review and document **Delta Security Best Practice** items		GS
Review and document **Security Metrics**		GS
Review and document **Delta Critical Updates** (Customer Action) items		GS
Review and document **Delta Instance Scan** (Best Practice) non-compliant Items		GS
Review and document **Delta Data Privacy** Items		GS
Review and document **Delta Licensing** Items		GS
Update Baseline 1 for Dev		GS
Assess: Test Instance	**Client**	**GetSome**
Update **Security Center Application**		GS
Execute **Instance Hardening** scan		GS
Execute **Additional Security Checks** scan checks		GS
Execute **Full Instance Scan**		GS
Perform **Manual checks**		GS

Review and document **Delta Instance Hardening** non-compliant items		GS
Review and document **Delta Additional Security** non-compliant items		GS
Review and document **Delta Security Best Practice** items		GS
Review and document **Security Metrics**		GS
Review and document **Delta Critical Updates** (Customer Action) items		GS
Review and document **Delta Instance Scan** (Best Practice) non-compliant Items		GS
Review and document **Delta Data Privacy** Items		GS
Review and document **Delta Licensing** Items		GS
Update Baseline 1 for Test		GS
Assess: Staging Instance	**Client**	**GetSome**
Update **Security Center Application**		GS
Execute **Instance Hardening** scan		GS
Execute **Additional Security Checks** scan checks		GS
Execute **Full Instance Scan**		GS
Perform **Manual checks**		GS
Review and document **Delta Instance Hardening** non-compliant items		GS
Review and document **Delta Additional Security** non-compliant items		GS
Review and document **Delta Security Best Practice** items		GS
Review and document **Security Metrics**		GS
Review and document **Delta Critical Updates** (Customer Action) items		GS
Review and document **Delta Instance Scan** (Best Practice) non-compliant Items		GS
Review and document **Delta Data Privacy** Items		GS
Review and document **Delta Licensing** Items		GS
Update Baseline 1 for Staging		GS
Assess: Production Instance	**Client**	**GetSome**
Deploy Change for Production Security Center Update: **DD/MMM**		GS
Update **Security Center Application**		GS
Execute **Instance Hardening** scan		GS
Execute **Additional Security Checks** scan checks		GS
Execute **Full Instance Scan**		GS
Perform **Manual checks**		GS
Review and document **Delta Instance Hardening** non-compliant items		GS
Review and document **Delta Additional Security** non-compliant items		GS
Review and document **Delta Security Best Practice** items		GS
Review and document **Security Metrics**		GS
Review and document **Delta Critical Updates** (Customer Action) items		GS

Review and document **Delta Instance Scan** (Best Practice) non-compliant Items		GS
Review and document **Delta Data Privacy** Items		GS
Review and document **Delta Licensing** Items		GS
Update Baseline 1 for Prod		GS
Report	**Client**	**GetSome**
Investigation of Prod findings		GS
Investigation of Staging findings		
Investigation of Test findings		GS
Investigation of Dev findings		GS
Produce Assessment Report		GS
Monthly Meeting: DD/MMM - 0.5 hours duration	**Client**	**GetSome**
Facilitate Monthly Review meeting		GS
Review Assessment Checklist and Report with client	PC, PO, ADM	GS
Update Baseline 1 - with agreed remediation items		GS
Confirm Assessment Phase Items Complete		GS
Decide upon remediation approach	PC	GS
Exit Criteria		
Confirmation from GS that Assessment Phase items have completed		GS
Remediation approach understood	PC	
Project Change Request document signed by both parties (optional - required for additional Remediation time)	PC	GS
Outputs		
Assessment Report, Recommended Remediation Items, Decision on Remediation approach, Project Change Request document (optional)		
Phase - Remediate - Duration 2 days (monthly)		
Entry Criteria		
Assess Phase complete		
Inputs		
Assessment Report, Recommended remediation items, Draft Changes, Draft Remediation Plan		
Task	**Resources (Responsible)**	
Identify UAT testers	PC**	GS
Remediate Development Instance	**Client**	**GetSome**
Develop common fixes (Update sets, data files and process steps)		GS
Develop unique fixes (done on point basis)		GS
GetSome testing		GS

UAT Development Instance	**Client**	**GetSome**
Request UAT where appropriate	PC	GS
Perform UAT	PC**	GS
Obtain signoff on UAT	PC	GS
UAT Defect remediation	PC**	GS
Documentation	**Client**	**GetSome**
Update As Built documentation		GS
Approve As Built documentation	PC	
Update Baseline	**Client**	**GetSome**
Rescan environment - Hardening, Additional Security, Full Instance		GS
Update Baseline 1		GS
Remediate Test Instance	**Client**	**GetSome**
Develop common fixes (Update sets, data files and process steps)		GS
Develop unique fixes (done on point basis)		GS
GetSome testing		GS
UAT Test Instance	**Client**	**GetSome**
Request UAT where appropriate	PC	GS
Perform UAT	PC**	GS
Obtain signoff on UAT	PC	GS
UAT Defect remediation	PC**	GS
Documentation	**Client**	**GetSome**
Update As Built documentation		GS
Approve As Built documentation	PC	
Update Baseline	**Client**	**GetSome**
Rescan environment - Hardening, Additional Security, Full Instance		GS
Update Baseline 1		GS
Remediate Staging Instance	**Client**	**GetSome**
Develop common fixes (Update sets, data files and process steps)		GS
Develop unique fixes (done on point basis)		GS
GetSome testing		GS
UAT Staging Instance	**Client**	**GetSome**
Request UAT where appropriate	PC	GS
Perform UAT	PC**	GS
Obtain signoff on UAT	PC	GS
UAT Defect remediation	PC**	GS
Documentation	**Client**	**GetSome**
Update As Built documentation		GS
Approve As Built documentation	PC	
Update Baseline	**Client**	**GetSome**

Rescan environment - Hardening, Additional Security, Full Instance		GS
Update Baseline 1		GS
Remediate Production Instance	**Client**	**GetSome**
Develop unique fixes (done on point by point basis)		GS
Deploy common fixes (Low Risk Change)		GS
Deploy common fixes (n x Additional Changes)		GS
GetSome testing		GS
UAT Production Instance	**Client**	**GetSome**
Request UAT where appropriate	PC	GS
Perform UAT	PC**	GS
Obtain signoff on UAT	PC	GS
UAT Defect remediation	PC**	GS
Documentation	**Client**	**GetSome**
Update As Built documentation		GS
Approve As Built documentation	PC	
Update Baseline	**Client**	**GetSome**
Rescan environment - Hardening, Additional Security, Full Instance		GS
Update Baseline 1		GS
Update meeting: DD/XXX - 0.5 hr duration	**Client**	**GetSome**
Facilitate Closeout meeting		GS
Review Baseline 1 Delta and Report with client	PC, PO, ADM	GS
Confirm Remediation Phase Items Complete		GS
Exit Criteria		
Confirmation from GS that Remediation Phase items have completed		GS
Project Change Request document signed by both parties (required for additional Remediation Services)	PC	GS
Outputs		
Baseline 1, As Built documentation, Project Change Request document (optional)		

** Primary Contact responsible for providing UAT signoff