

Integrate InsightVM with ServiceNow Security Operations

The Rapid7 Integration for Security Operations allows you to incorporate InsightVM vulnerability assessment data into your ServiceNow Security Operations instance using a purpose-built API. You can then consume this data with dashboards and other ServiceNow analytics tools.

With this integration, you can:

- Import Rapid7 InsightVM scan data directly into ServiceNow Security Operations.
- Gain more context and visibility into individual vulnerabilities and overall risk.
- Reduce exposure time through data-centric collaboration between IT Operations and Security.
- Maximize output while minimizing effort through an automated and closed-loop workflow.
- Easily deploy the integration from the ServiceNow Marketplace.

How this integration works

Here's a high-level overview of how this integration works:

1. InsightVM scans your environment to assess your assets' level of risk and processes the vulnerability data.
2. ServiceNow Security Operations (SecOps) periodically queries InsightVM for the latest vulnerability information.
3. ServiceNow creates remediation tickets for vulnerabilities and closes tickets that have been fixed.
4. With future queries of InsightVM, ServiceNow checks closed tickets for successful remediation.

API request characteristics

If you prefer to include unchanged vulnerabilities that fall within the `currentTime` and the `comparisonTime` in the response, specify the `includeSame=true` parameter in the request.

To ensure that you're best set up for success with this integration, Rapid7 recommends the following configuration best practices:

- ## Supported search filters

Asset filters

Requirements

Before you get started with this integration, verify that you meet the following requirements.

Network traffic rules for the Insight Platform

Is your Rapid7 product subscription provisioned for the United States? Check your region code first!

As of April 12th, 2021, all new customers subscribing to Rapid7 Insight products that elect to store their data in the United States will be provisioned for one of three data centers. Since these data centers have unique endpoints, any firewall rules you configure must correspond to the data center your organization is assigned to. Follow these steps to determine which United States data center your organization is part of:

1. Go to insight.rapid7.com and sign in with your Insight account email address and password.
2. Navigate to the Platform Home page.
 - If you are not taken to this page by default, expand the product dropdown in the upper left and click **My Account**.
3. Look for the Data Storage Region tag in the upper right corner of the page below your account name. Your United States region tag will show one of the following data centers:
 - United States - 1
 - United States - 2
 - United States - 3

For ServiceNow to retrieve data from InsightVM, your network must allow outbound traffic to the hostname that corresponds to your current InsightVM data region. The following table contains hostnames for each of the current InsightVM data regions:

Region	Hostname
United States - 1	us.api.insight.rapid7.com
United States - 2	us2.api.insight.rapid7.com
United States - 3	us3.api.insight.rapid7.com
Canada	ca.api.insight.rapid7.com
Europe	eu.api.insight.rapid7.com
Japan	ap.api.insight.rapid7.com

<https://www.linkedin.com/in/mohammed-khadeer>

Region	Hostname
Australia	au.api.insight.rapid7.com

Make sure to configure your network for the correct region!

The region that houses your InsightVM data depends entirely on what region was selected during your InsightVM deployment. The network rule you configure here must correspond to the data region you selected previously in InsightVM, or this integration will be unable to retrieve any data.

Rapid7 API key

Your Rapid7 API key allows ServiceNow to request data from your InsightVM environment. For your API key to be usable with this integration, it must be generated by an Insight Platform user with the Platform Administrator role.

We'll cover how to generate your API key in the [deployment](#) procedure.

System requirements

The integration has several system requirements that you must satisfy, including installed plugins and user roles. You can review these requirements on the integrations' ServiceNow Store page:

https://store.servicenow.com/sn_appstore_store.do#!/store/application/8a2aa078e7330300809a268b03f6a988

Deployment

Complete the following steps to deploy the Rapid7 Integration for Security Operations.

Generate your API key

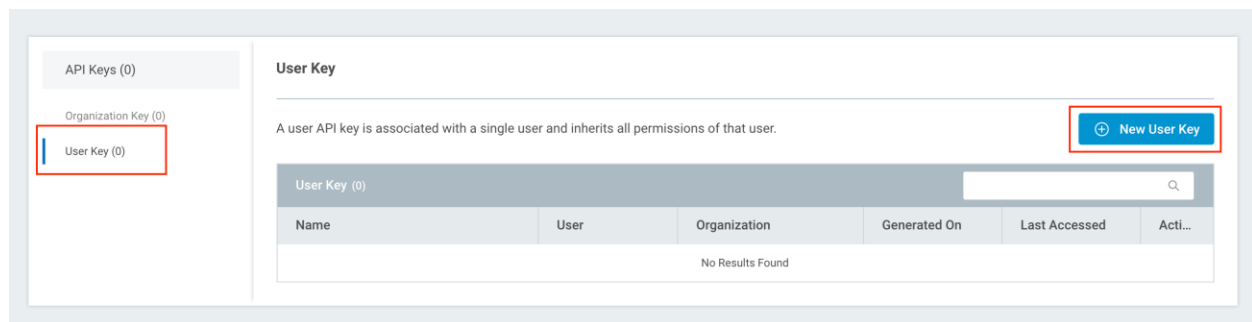
Platform Administrator role required

As a reminder, you must generate your API key with an Insight Platform user that has the Platform Administrator role. API keys generated by Insight Platform users in other roles will not be usable with this integration.

Follow these steps to generate your API key:

<https://www.linkedin.com/in/mohammed-khadeer>

1. Go to insight.rapid7.com and sign in with your Insight account email address and password.
2. Click the **API Key Management** tab on your left menu.
3. On the API Keys page, switch to the **User Key** view and click **+ New User Key**.



4. On the Generate New User Key panel, select the organization to which your InsightVM deployment belongs from the dropdown list.
5. Finally, give your API key a name for reference purposes. Click **Generate** to finish.
6. With your API key generated, copy and save the key in a secure location.

This is your only chance to copy this API key!

For security purposes, your API key will not be viewable again after this opportunity. Make sure you copy and save it now.

If you inadvertently skip this step, you can always generate a new API key.

7. Click **Done** after copying your API key. The key record will now appear by name in your User Key table.

Install and configure the integration

Now that you have your API key handy, follow these steps to access and install the Rapid7 Integration for Security Operations in ServiceNow:

1. Go to the [Rapid7 Integration for Security Operations page](#) in the ServiceNow store to add the integration to your ServiceNow application.
 - As covered in the requirements, this store page details the plugins and permissions you must already have installed to run the integration. For guidance on installing the integration app itself, see the [Install and configure the Rapid7 Integration for Security Operations application](#) ServiceNow document.

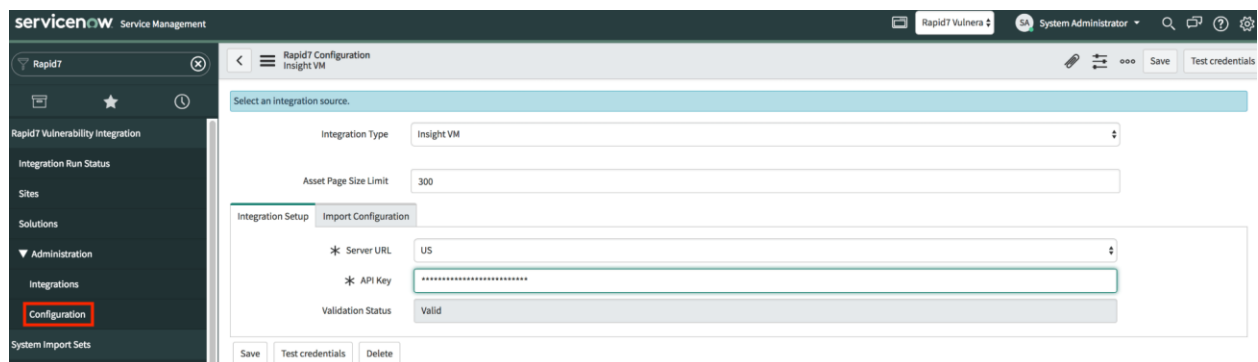
Integration types

The ServiceNow document listed previously details separate procedures for two integration types:

- InsightVM integration type
- Data warehouse integration type

The procedures in this article are meant for the InsightVM integration type.

2. After installing the integration, log in to your ServiceNow application and navigate to the **Rapid7 Vulnerability Integration** on your left menu.
3. Expand the **Administration** dropdown and click **Configuration**.
4. Select **InsightVM** from the Integration Type dropdown.
5. On the **Integration Setup** tab, select the region that corresponds to your InsightVM data region from the Server URL dropdown.
6. Paste your API key in the provided field.



The screenshot shows the ServiceNow interface for configuring the Rapid7 Vulnerability Integration. The left sidebar shows the 'Administration' dropdown expanded, with 'Configuration' highlighted. The main content area is titled 'Rapid7 Configuration Insight VM'. It features a 'Select an integration source.' section with a dropdown for 'Integration Type' set to 'Insight VM' and a text field for 'Asset Page Size Limit' set to '300'. Below this is the 'Integration Setup' section with an 'Import Configuration' tab. It contains a 'Server URL' dropdown set to 'US', an 'API Key' field with masked characters, and a 'Validation Status' field showing 'Valid'. At the bottom are 'Save', 'Test credentials', and 'Delete' buttons.

7. Click **Test Credentials** to verify that the integration is configured correctly and can communicate with InsightVM.
 - If the credential test succeeds, the Validation Status field will display Valid. Click **Save** to finish your integration deployment.
 - If the credential test fails, verify that you've configured your network traffic rules for the correct data region and check that your Server URL and API Key values are input correctly before trying again.

Rapid7 Integration for Security Operations deployment complete!

InsightVM data will now appear in your ServiceNow application to help manage your remediation efforts.

Frequently asked questions

The following sections contain answers to some frequently asked questions about this integration and how it works.

I'm getting asset inventory data, but no vulnerability data on those assets. Why is this happening?

Make sure that you are setting a `comparisonTime` value in your query. Without this value, there is no date and time to run a comparison against. Consequently, the API will only return vulnerabilities that were new since the `currentTime` of your query, which is either the current time as set in the API request or the moment the request is executed. Additionally, the API only returns lists of new and remediated vulnerabilities. If a vulnerability is present that was also present at the time you were comparing against, this vulnerability will not appear in the response. If you've set a `comparisonTime` and there are no new or remediated vulnerabilities coming back from the endpoint as expected, contact the Rapid7 Support team.

I'm trying to get all remediated vulnerabilities on an asset using a very old `comparisonTime` and a very recent `currentTime`, but they aren't appearing. Why is this happening?

Make sure that you're setting a `comparisonTime` at a point where the asset you want to query for actually existed. If the asset did not exist at the `comparisonTime` you specified, there won't be any vulnerabilities that existed at that time either. Consequently, there will be no remediated vulnerabilities to return at the `currentTime` if no vulnerabilities existed at the `comparisonTime`.

If the number of total vulnerabilities is greater than 0, why don't I see any vulnerabilities in the "New" or "Remediated" list?

The API does not include unchanged vulnerabilities (meaning those vulnerabilities that are currently found on an asset that were already present during the last scan) in the response unless you set a parameter manually in the request that exposes this information. The total number of vulnerabilities is still correct; unchanged vulnerabilities are just hidden by default. You can modify your request with the `includeSame=true` parameter to expose those unchanged vulnerabilities in the response.

How is the "Remediated" date for a vulnerability on the remediated list calculated?

The API defines the remediation time for a vulnerability as the first date when an asset was scanned and that particular vulnerability was not found.

My response is missing some information. What happened?

If an asset or vulnerability does not have a certain property (such as asset tags or similar optional properties), that property will not appear in your response.

What is the cursor and how do I use it?

The `cursor` parameter allows you to search through sorted data in large responses. For example, if your API request produces a response that includes a `cursor` parameter value itself, you can then make another request that specifies this `cursor` value to retrieve the next page of data. Remember that `cursor` parameters are very specific to the exact queries that generate them. If your request produces a cursor and you intend to use it, your next request must exactly match the query criteria you used previously (the only difference being that you are providing the previously returned `cursor` value in the second request).

What are the recommended maximum page sizes?

Rapid7 recommends a page maximum of 100 for assets and 500 for vulnerabilities. If your requests also specify `includeSame=true`, set the page maximum to 50 for assets. When using a Vulnerability filter we recommend setting the request size to 25 as this filter type can impact performance. Request size can remain at 50 if no filters are applied or if only the asset filter is applied. Response times will vary depending on the amount of data that is retrieved for each request.

What format are responses in?

Responses can be formatted in JSON or XML depending on what you configure in the request header.

What vulnerability metrics does the API use?

The API uses both [vulnerability finding metrics](#) and [vulnerability instance metrics](#). Each vulnerability instance includes the vulnerability proof, the vulnerability check that was used, and other relevant information. Each asset will report the total number of

vulnerability findings. If new instances are found or remediated, those will be listed as well.

Can I generate a report from my InsightVM dashboard to use as a baseline comparison between ServiceNow Security Operations and InsightVM?

Yes. In InsightVM, go to any expandable, global vulnerability-based card (such as Vulnerabilities By CVSS Score) and export the entire table's contents as a CSV file. Import this CSV file into whatever spreadsheet software you have available and calculate the sum of the Instances column. You can compare this value to the figure shown in the Detection table in ServiceNow Security Operations.

Can I combine data from this integration with data from the data warehouse integration in the ServiceNow product itself?

No. The two integrations are completely separate from each other. If both integrations are options for deployment in your environment, choose one (and only one) to be used with ServiceNow.

How does ServiceNow handle deleted assets in InsightVM?

Assets that are deleted from InsightVM will no longer be returned by the API with subsequent requests. As a result, the corresponding asset in ServiceNow Security Operations will become stale. ServiceNow has its own retention policy that can address this scenario by removing asset records that have not been updated after a configured number of days. Consult your ServiceNow product documentation for instructions.