

Dashboard

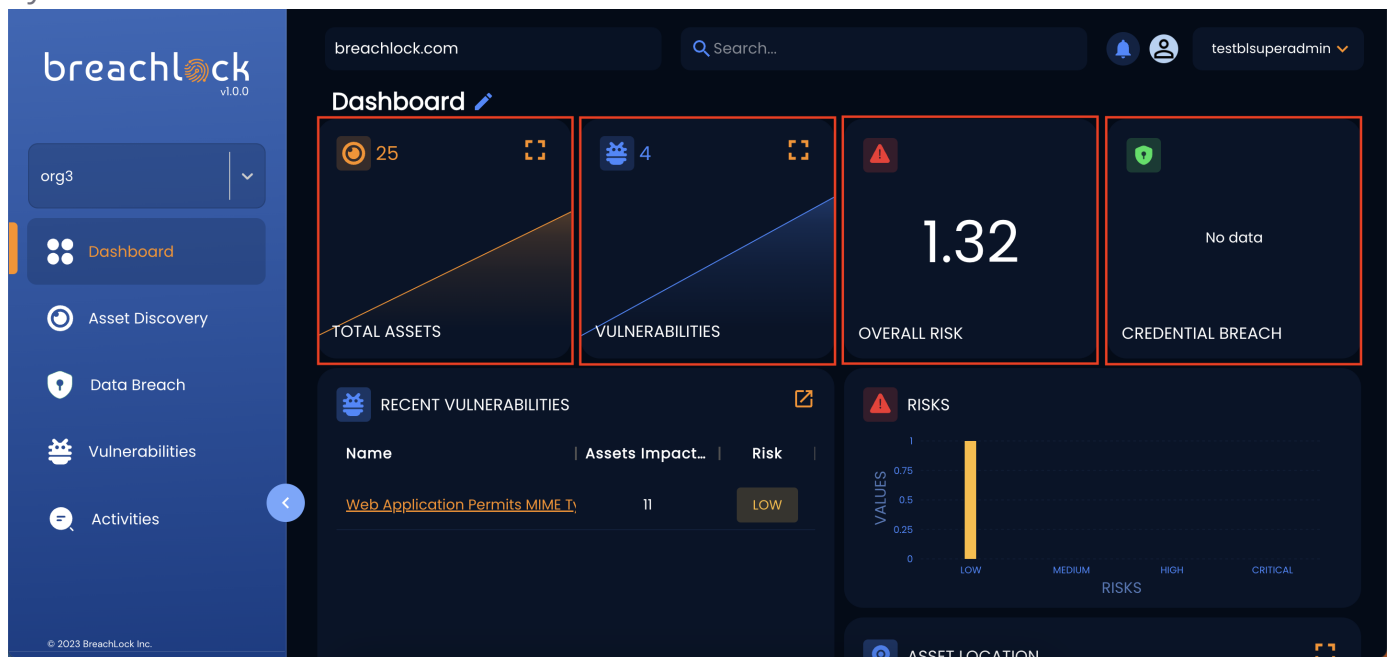
This section will allow you to clarify your queries about the dashboard and the widgets available to your organization.

You can view the default dashboard widget details: [Dashboard Widgets](#)

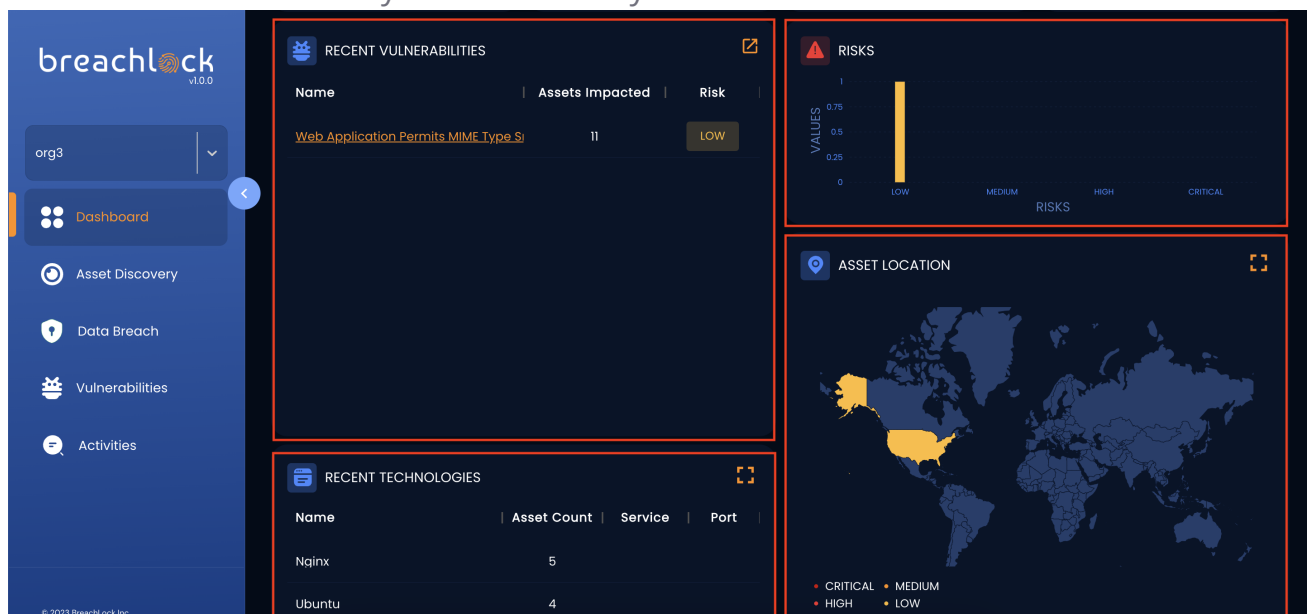
If you want to customize the dashboard for yourself, you can clarify your doubts here: [Customize Widgets](#)

Dashboard Widget

You can view the following widgets in the ASM platform; these widgets are available to you by default. Here are the details:



- **Total Assets:** This widget will show your organization's total assets and the trend graph for the growth/decline
- **Credential Breach:** This widget will show your organization's total credential breaches and the trend graph for the growth/decline.
- **Vulnerabilities:** This widget will show your organization's total vulnerabilities and the trend graph for the growth/decline.
- **Overall Risk:** This widget will show the highest level of risk that the organization has and how many vulnerabilities there are in this risk category.
- **Top Vulnerability List:** This widget will show the top vulnerabilities(Name and their risk) and the assets affected by the vulnerability.



- Value to Risk Category Ratio: This widget will show the different categories of risk and the number of vulnerabilities in each risk category.
- Asset Location: This widget will show the asset location based on criticality in a map view.
- Technologies Widget: This will show the different types of technologies that your organization has used and if they are at risk.

You can add or remove widgets from the default layout per your requirements. To learn more about the customization of widgets, please refer to [Widget Customization](#)

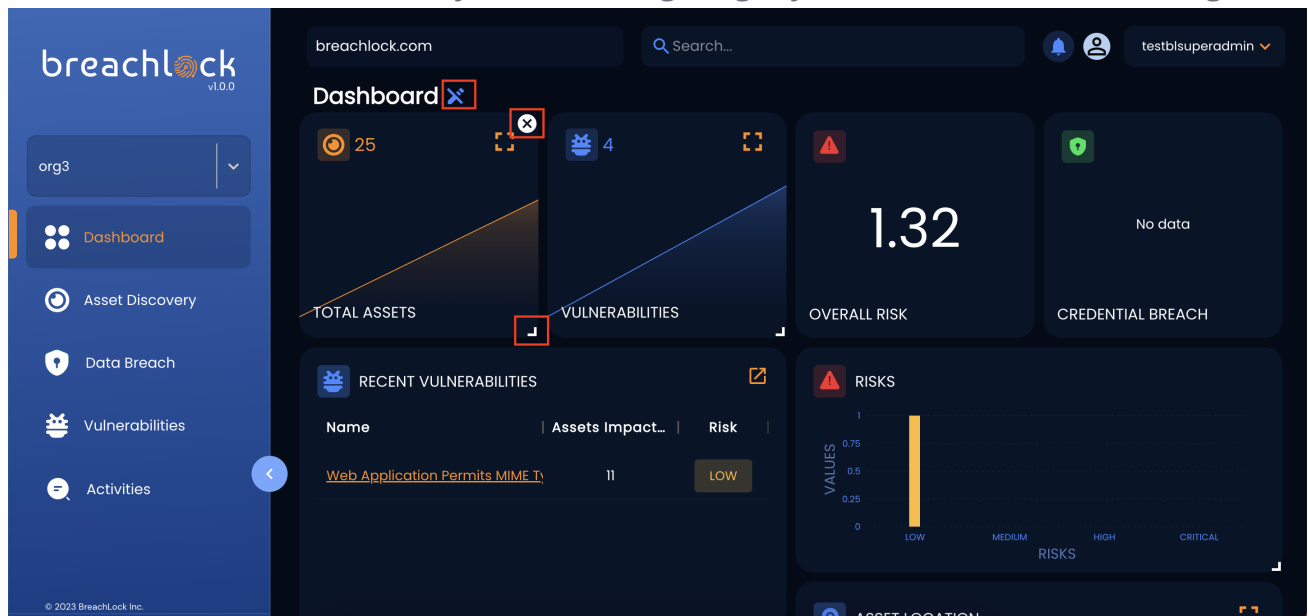
Dashboard Widget Customization

Here you can go through how you can customize the widgets or layout of your dashboard. The customization will only be for your account, not the whole organization. Here are the things you can do:

- On the dashboard, click the edit button to change the widgets or layout.



- You can change the size of the widgets or change the place of the widgets. If the size is increased or decreased, the layout will change slightly to accommodate the change.



- You can also reset the dashboard to default or add new widgets from the available list.
- Once you save the changes, the dashboard will be updated for your account. These changes will only reflect on your account and not on anyone else in your organization.

Assets Discovered

This section will introduce you to the assets discovered module in the platform. Here you will go through all assets that are being identified by the platform.

To learn more about different assets that are discovered: [Asset Details](#)

To understand how you can mark an asset as a false positive / archive if there are assets on which you don't want to run future scans: [Mark False Positive](#)

To understand how you can manually run a scan: [Run Scan](#)

Asset Details

This section will introduce you to different types of assets discovered by the platform and what information will be available to you and your organization. You can check the following discovered assets for the organization:

- Sub Domains: Here, you can see the list of Sub Domain that have been found for your organization. The data will be shown in a table view. In the table, you will see the name of Sub Domain, Hosted status, IP count, DNS count and Created Date.

The screenshot shows the BreachLock v1.0.0 interface. On the left is a sidebar with navigation links: Dashboard, Asset Discovery (highlighted), Data Breach, Vulnerabilities, and Activities. The main area is titled 'Asset Discovery' and shows a search bar, a filter for 'True Positive', and a table of subdomains. The table has columns: Name, Scan Status, Hosted, IP Count, DNS Co..., Vulnerabili..., and Updated At. The subdomains listed are event-demo.breachlock.com, cirrus.breachlock.com, vids-acc.breachlock.com, gpp-acc.breachlock.com, and vids.breachlock.com. The 'Hosted' column shows 'Yes' for all, and the 'Updated At' column shows dates from 06-20-2023T14:21 to 06-20-2023T14:19.

Name	Scan Status	Hosted	IP Count	DNS Co...	Vulnerabili...	Updated At
event-demo.breachlock.com	Finished	Yes	1	2	3	06-20-2023T14:21
cirrus.breachlock.com	W N	Yes	1	2	3	06-20-2023T14:20
vids-acc.breachlock.com	W N	Yes	4	6	2	06-20-2023T14:20
gpp-acc.breachlock.com	W N	Yes	4	6	2	06-20-2023T14:20
vids.breachlock.com	W N	Yes	4	6	2	06-20-2023T14:19

- They can also view the asset details and what IP addresses, DNS, vulnerabilities and activities with the finding details.

The screenshot shows the 'Subdomain Details' page for event-demo.breachlock.com. It has tabs for IP Address (1), DNS (2), Vulnerability (3), and Activities (2). The 'Vulnerability' tab is selected, showing a list of findings. The first finding is 'Fully Qualified Domain Name (FQDN) Resolved' with a CVSS Score of 0. The details show that the remote host is resolved in the fully qualified domain name (FQDN): ec2-34-212-189-161.us-west-2.compute.amazonaws.com. The host is event-demo.breachlock.com, and the findings were updated at 06-20-2023T14:21. The second finding is 'Web Application Does Not Supply a Referrer Policy' with a CVSS Score of 0. The third finding is 'Web Application Does Not Supply a Permissions Policy' with a CVSS Score of 0.

- IP Address: Here, you can see your organization's list of IP addresses. The data will be shown in a table view. The table shows the IP address's name, Country, Organization,

subdomain count and Created Date.

The screenshot displays the BreachLock Asset Discovery interface. The left sidebar contains a navigation menu with 'Asset Discovery' highlighted. The main panel shows a table of IP Assets. The table has columns: Name, Scan Status, Hosted, IP Count, DNS Count, Vulnerability, and Updated At. Two rows are visible: 192.124.249.161 and 18.164.144.67. The 'IP Assets' tab is selected, showing 2 assets. The 'Subdomains' tab shows 27 subdomains and 'IP Blocks' shows 23 blocks.

Name	Scan Status	Hosted	IP Count	DNS Count	Vulnerability	Updated At
192.124.249.161	(W) (N)	Yes	4	5	2	05-28-2023T09:51
18.164.144.67	(W) (N)	Yes	1	1	4	05-27-2023T20:40

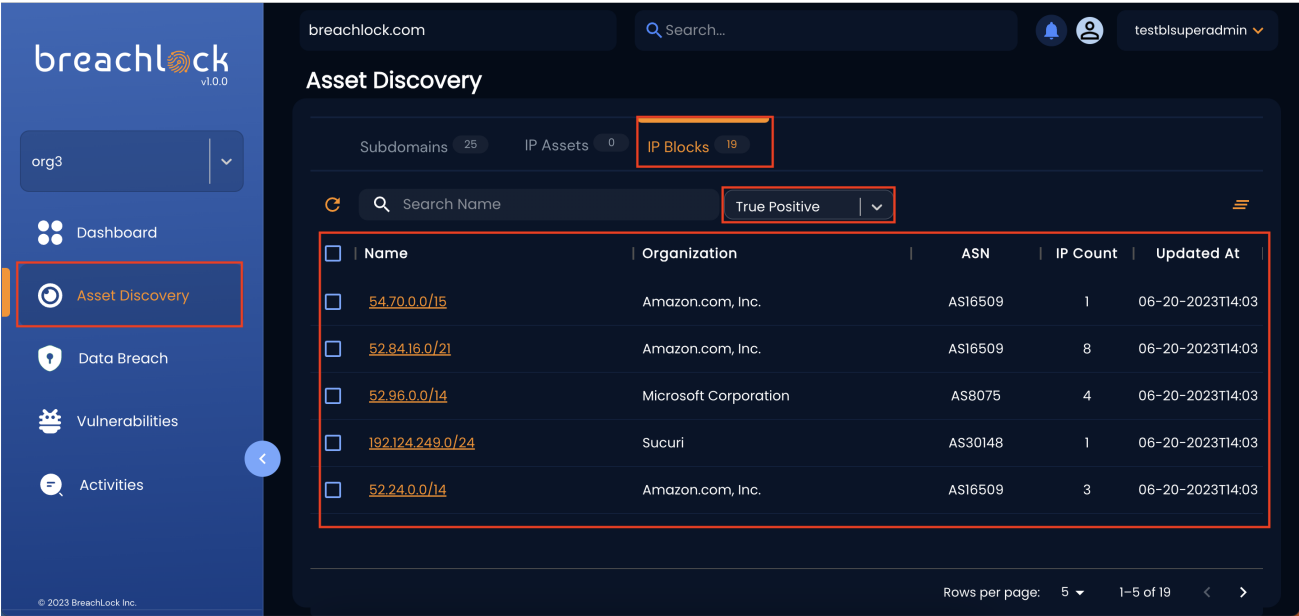
- o They can also view the asset details and what subdomains, IP Blocks, vulnerabilities and activities with the finding details.

The screenshot displays the BreachLock IP Assets Details interface. The main panel shows a list of vulnerabilities for the IP address 192.124.249.161. The list includes: Test Vulnerability LOW (CVSS Score: 0), Test Vulnerability MEDIUM (CVSS Score: 3), Test Vulnerability HIGH (CVSS Score: 6), and Test Vulnerability CRITICAL (CVSS Score: 9). The 'Vulnerability' tab is selected, showing 7 vulnerabilities. The 'IP Address' tab shows 4 IP addresses, 'DNS' shows 5 DNS records, and 'Activities' shows 1 activity.

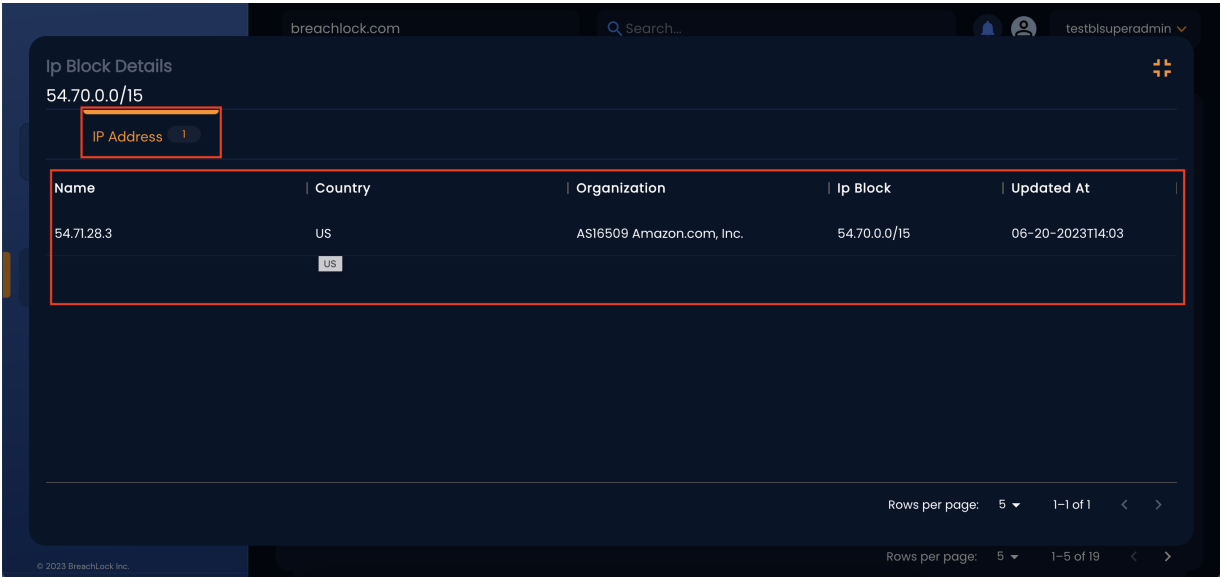
Test Vulnerability	Severity	CVSS Score
Test Vulnerability LOW	LOW	0
Test Vulnerability MEDIUM	MEDIUM	3
Test Vulnerability HIGH	HIGH	6
Test Vulnerability CRITICAL	CRITICAL	9

- IP Block: Here, you can see the list of IP Blocks that have been found for your organization. The data will be shown in a table view. In the table, you will see the name

of the IP block, asn count and Created Date.



- They can also view the asset details and what IP addresses with the finding details.



You can also view the details of the assets. The assets affected by vulnerability will have the option to view the details of the asset, what vulnerabilities are there in the asset, when the vulnerability was found, and the updated time.

False Positive

This section will introduce you to the functionality of marking an asset as a false positive. You can mark an asset as false positive by selecting the checkbox in the table for any asset.

breachlock
v1.0.0

org3

Dashboard

Asset Discovery

Data Breach

Vulnerabilities

Activities

© 2023 BreachLock Inc.

breachlock.com

Search...

testblsuperadmin

Asset Discovery

Subdomains 25

IP Assets 0

IP Blocks 19

False Positive

Run Scan

	Name	Scan Status	Hosted	IP Count	DNS Co...	Vulnerabili...	Updated At
<input checked="" type="checkbox"/>	event-demo.breachlock.com	<div>W</div> <div>N</div>	Yes	1	2	3	06-20-2023T14:21
<input type="checkbox"/>	cirrus.breachlock.com	<div>W</div> <div>N</div>	Yes	1	2	3	06-20-2023T14:20
<input type="checkbox"/>	vids-acc.breachlock.com	<div>W</div> <div>N</div>	Yes	4	6	2	06-20-2023T14:20
<input type="checkbox"/>	app-acc.breachlock.com	<div>W</div> <div>N</div>	Yes	4	6	2	06-20-2023T14:20
<input type="checkbox"/>	vids.breachlock.com	<div>W</div> <div>N</div>	Yes	4	6	2	06-20-2023T14:19

1 row selected

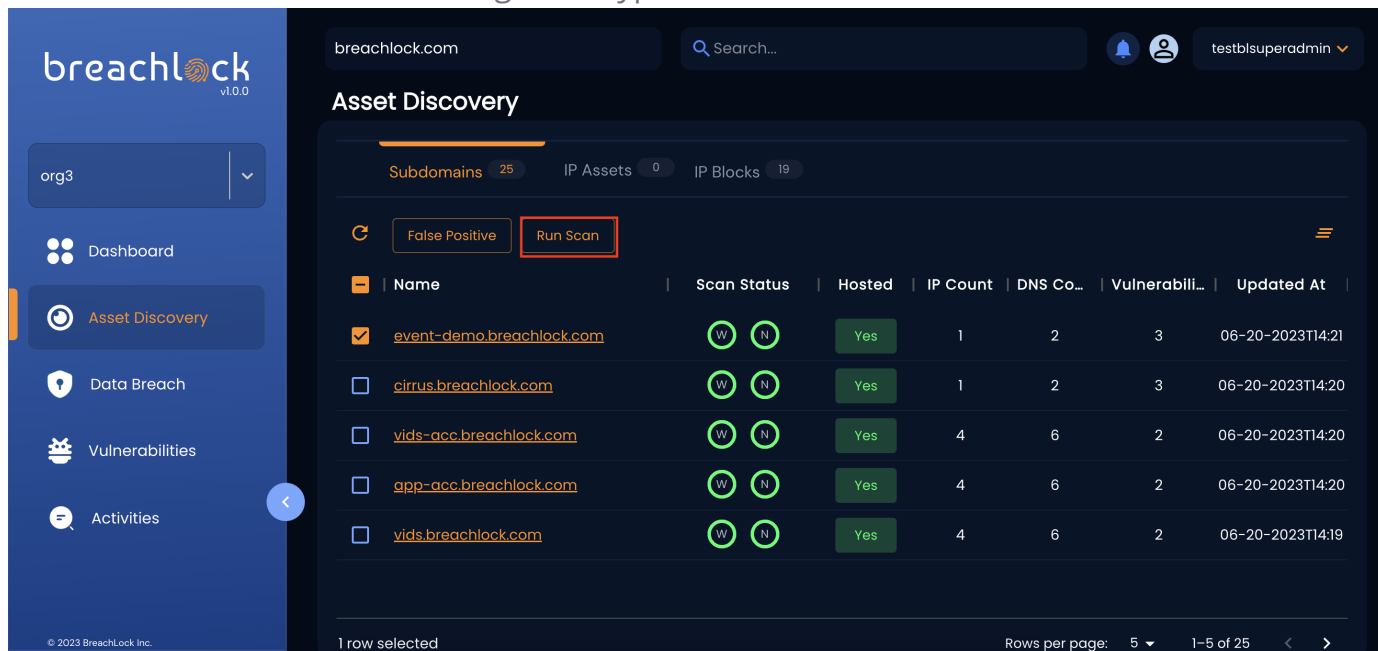
Rows per page: 5 1-5 of 25

If an asset is marked as false positive, it will be taken off the list and will go in the list of false positive assets, and no further scans will be run on these assets.

Run Scan

This section will introduce you to the manual running of scans on different assets.

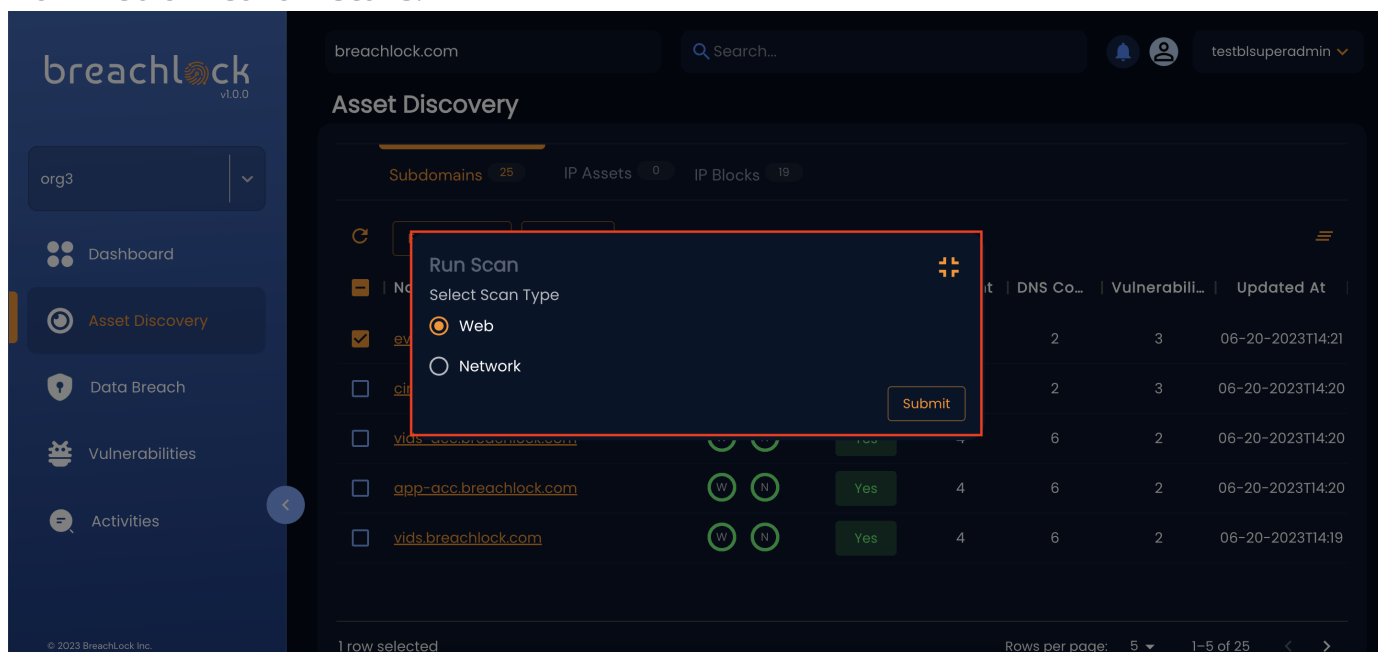
The scans for your organization usually run automatically(asset discovery scan) on the frequency set per your requirements. If you want to run a scan for vulnerabilities on an asset, you can also do that for IP addresses and Sub Domains. The option to run a scan will not be available for the remaining asset types.



The screenshot shows the BreachLock v1.0.0 interface. The left sidebar contains navigation links: Dashboard, Asset Discovery (selected), Data Breach, Vulnerabilities, and Activities. The main content area is titled 'Asset Discovery' and shows a list of subdomains. A red box highlights the 'Run Scan' button in the top right corner of the table. The table has columns: Name, Scan Status, Hosted, IP Count, DNS Co..., Vulnerabili..., and Updated At. The first row is selected, and the 'Run Scan' button is highlighted.

Name	Scan Status	Hosted	IP Count	DNS Co...	Vulnerabili...	Updated At
event-demo.breachlock.com	W N	Yes	1	2	3	06-20-2023T14:21
cirrus.breachlock.com	W N	Yes	1	2	3	06-20-2023T14:20
vids-acc.breachlock.com	W N	Yes	4	6	2	06-20-2023T14:20
app-acc.breachlock.com	W N	Yes	4	6	2	06-20-2023T14:20
vids.breachlock.com	W N	Yes	4	6	2	06-20-2023T14:19

If you run a manual scan on 1 or multiple assets, the count will decrease from the total scans that your company has. When running the scan, they will have the option to select from web or network scans.



The screenshot shows the BreachLock v1.0.0 interface with a 'Run Scan' modal dialog open. The dialog has a title 'Run Scan' and a subtitle 'Select Scan Type'. It contains two radio buttons: 'Web' (selected) and 'Network'. A 'Submit' button is at the bottom right. The background shows the same table of subdomains as the previous screenshot.

Name	Scan Status	Hosted	IP Count	DNS Co...	Vulnerabili...	Updated At
event-demo.breachlock.com	W N	Yes	1	2	3	06-20-2023T14:21
cirrus.breachlock.com	W N	Yes	1	2	3	06-20-2023T14:20
vids-acc.breachlock.com	W N	Yes	4	6	2	06-20-2023T14:20
app-acc.breachlock.com	W N	Yes	4	6	2	06-20-2023T14:20
vids.breachlock.com	W N	Yes	4	6	2	06-20-2023T14:19