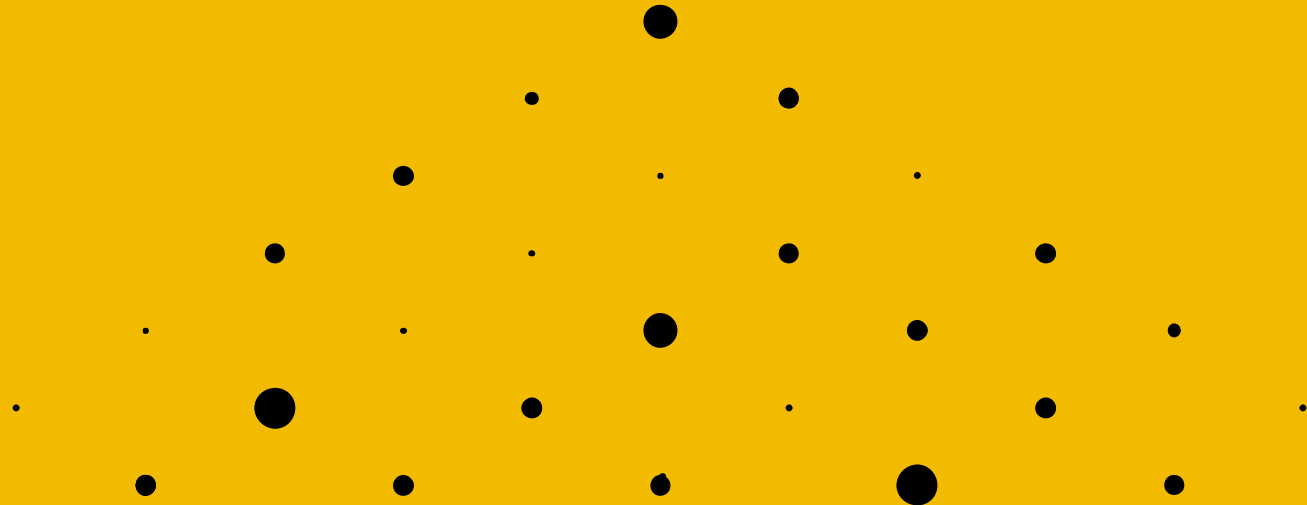


SiteZone Power BI Dashboard – Access and Analysis Instructions



Invite emails

First Invite - Azure

- **Action** – Click on ‘Accept invitation’
- **What does this do** – This adds your email address into the SiteZone (OnGrade) account. By accepting this invite it enables Power BI to share the dashboard with external users outside of the SiteZone organisation.
- **Tip: If you get asked for Microsoft Authentication please see slides 3-10**

Sender: Steve Dowding (Steve.Dowding@ongrade.com)
 Organisation: OnGrade Ltd
 Domain: sitezonesafety.com

If you accept this invitation, you'll be sent to https://account.activedirectory.windowsazure.com/?tenantid=4cf9518d-3a27-4695-ae20-226648f81a36&login_hint=

[Accept invitation](#)

[Block future invitations](#) from this organisation.

This invitation email is from OnGrade Ltd (sitezonesafety.com) and may include advertising content. OnGrade Ltd has not provided a link to their privacy statement for you to review. Microsoft Corporation facilitated sending this email but did not validate the sender or the message.

Microsoft respects your privacy. To learn more, please read the [Microsoft Privacy Statement](#).
 Microsoft Corporation, One Microsoft Way, Redmond, WA 98052



Second Invite – Power BI

- **Action** – Click on ‘Open this report’ & log in to you own Power BI account (this will be your Microsoft password)
- **What does this do** – This will open Power BI and direct you to the SiteZone dashboard report that has been shared with you.

Tip: Once you’ve opened the report, bookmark the link for easier access next time.

From: Microsoft Power BI <no-reply-powerbi@microsoft.com>
 Sent: 10 August 2022 10:46
 To: I
 Subject: Hubert Urbaniak has shared Power BI Report 'Customer - RCV Data V4' with you



Power BI

Hubert Urbaniak shared this Power BI Report with you

Customer - RCV Data V4

[Open this report > \[nam.safelink.emails.azure.net\]](#)



Download the Power BI app to access this report from your mobile device.



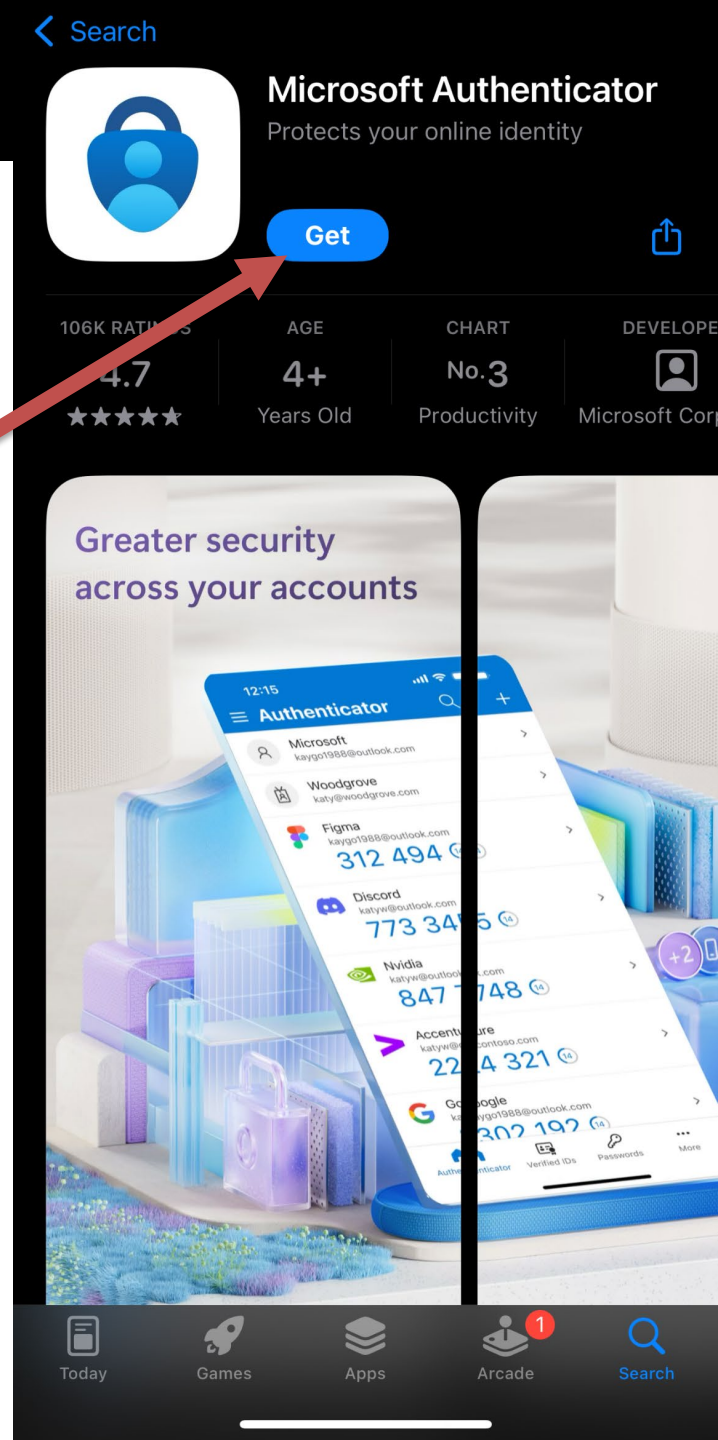
[\[nam.safelink.emails.azure.net\]](#)

[\[nam.safelink.emails.azure.net\]](#)

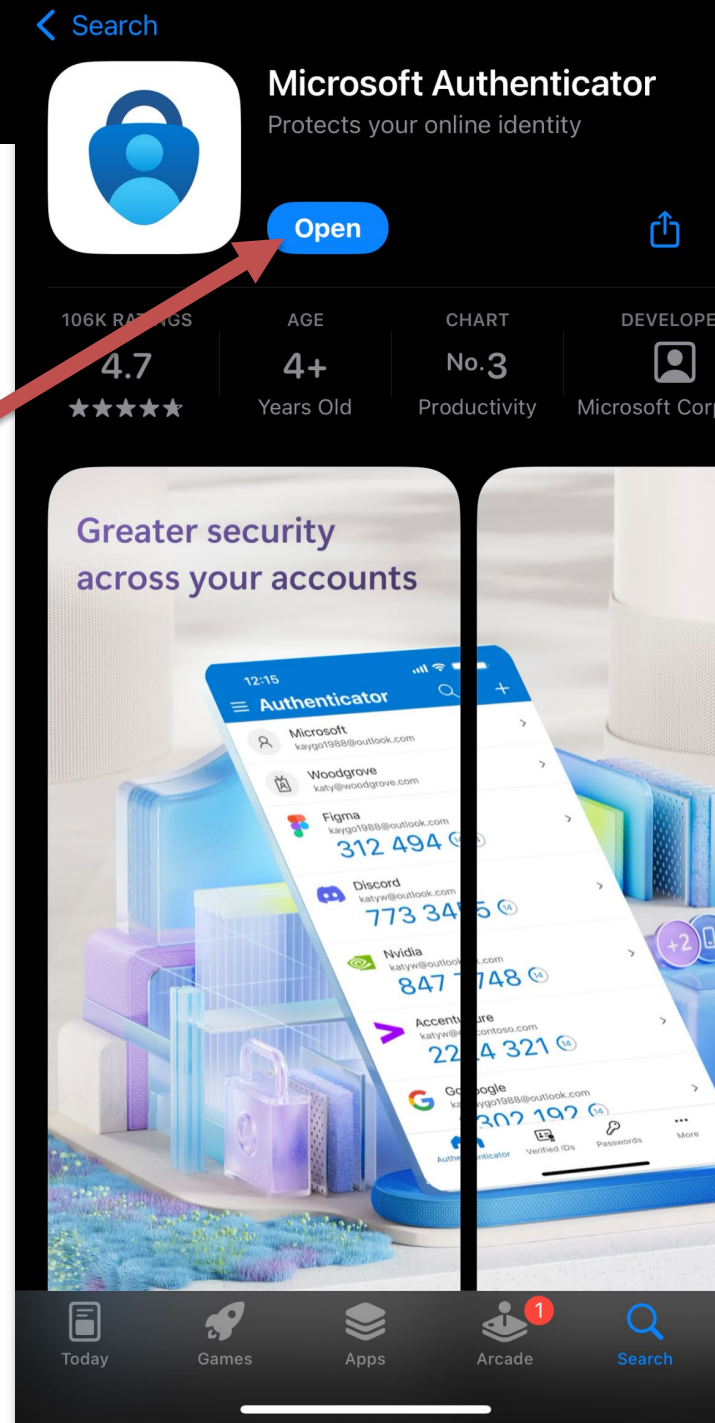
[\[nam.safelink.emails.azure.net\]](#)

A subscription to Microsoft Power BI Pro (payable directly to Microsoft) is required to access the SiteZone dashboard.

- Step 1: Download the Microsoft Authenticator App
1. Open the App Store (for iOS devices) or Google Play Store (for Android devices) on your smartphone.
 2. Use the search bar to type Microsoft Authenticator.
 3. Locate the app and tap the Download or Install button.



- Step 2: Open the App
- Once the installation is complete, tap Open from the app store or locate the app icon on your home screen and tap to open it.



- Step 3: Set Up the App



Microsoft respects your privacy

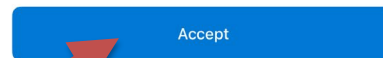
We collect required diagnostic data to keep the app secure and updated. This does not include any personal data.



Help us improve Microsoft Authenticator

By allowing us to collect additional non-personal data, you can help us improve the app. You can turn this on or off at any time in the Settings page

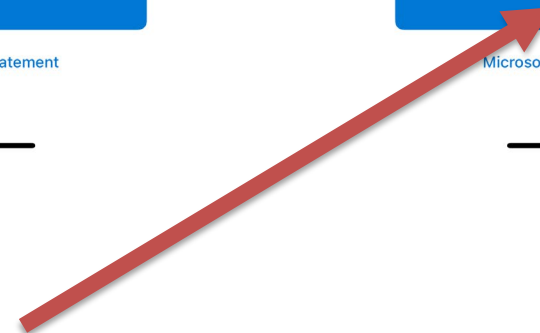
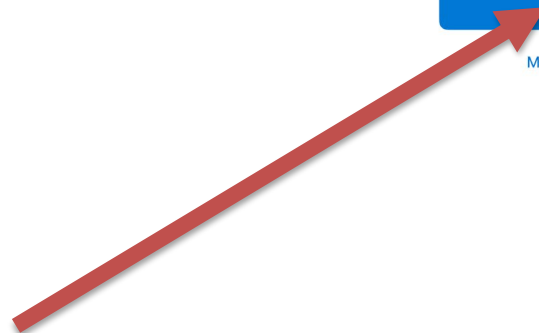
Help improve the app by sharing your app usage data



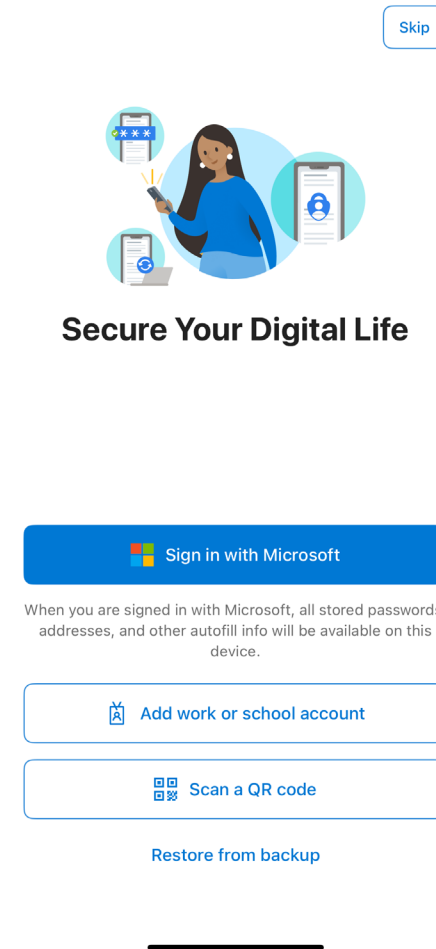
Microsoft Privacy Statement



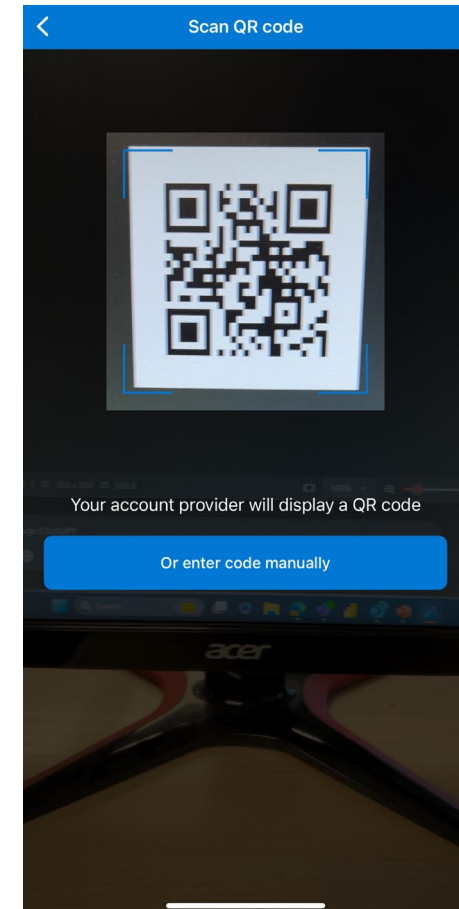
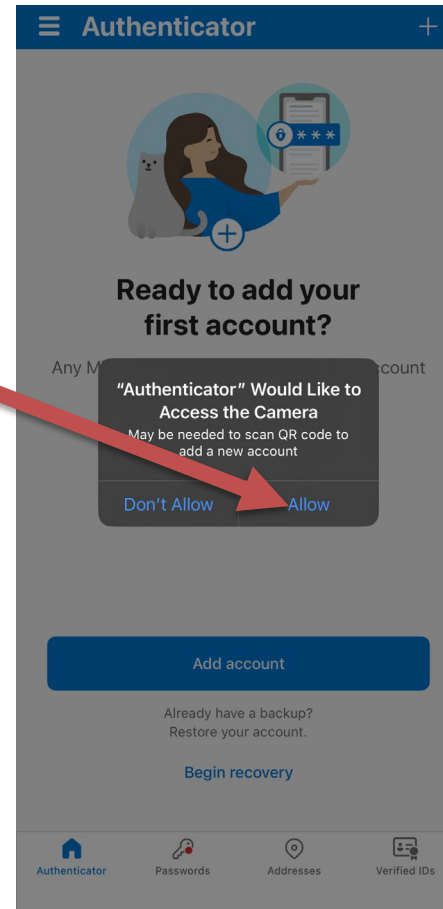
Microsoft Privacy Statement



- Step 4: Add Your First Account
- Choose an account type. Common options are:
 - Work or school account: For accounts managed by your organization.
 - Personal account: For Microsoft accounts like Outlook or Xbox.
- Follow the prompts to connect the app to your account.



- Step 5: Scan the QR Code
- On the welcome screen, you'll see an introduction to the app's features. Tap Get Started or Add Account (depending on your version).
- If prompted, allow the app to access your camera and send notifications.
- If you're setting up an account that uses two-factor authentication, a QR code will typically be provided by the service.
- On the app, select Scan QR Code. Point your camera at the QR code displayed on your computer or another device.
- If the QR code is unavailable, you may be able to enter a setup key manually.




- Step 6: Approve sign-in by preferred method

Cancel

 Microsoft

h m

Approve sign-in request

 Open your Outlook mobile app, and enter the number shown to sign in.

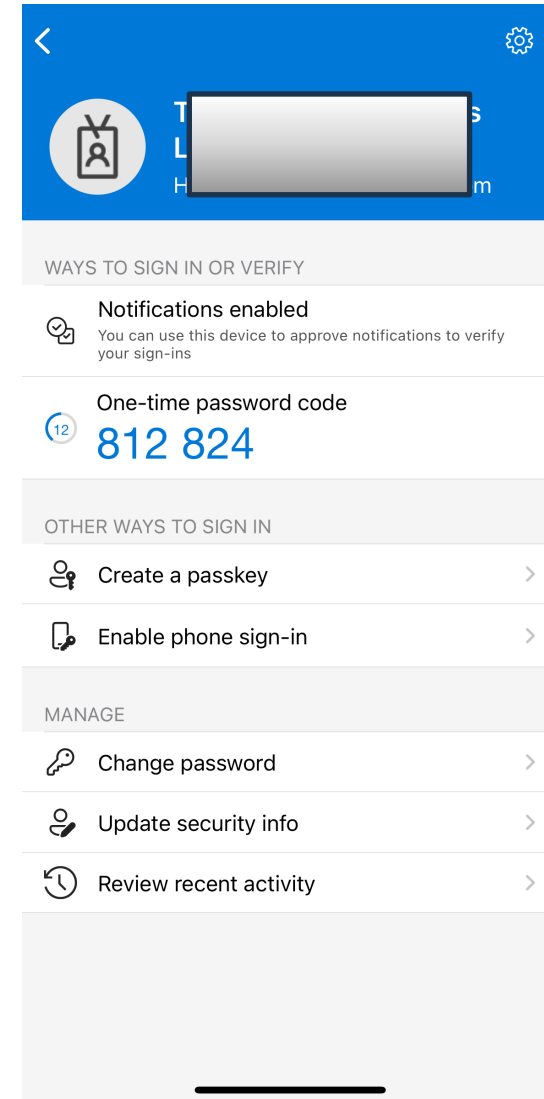
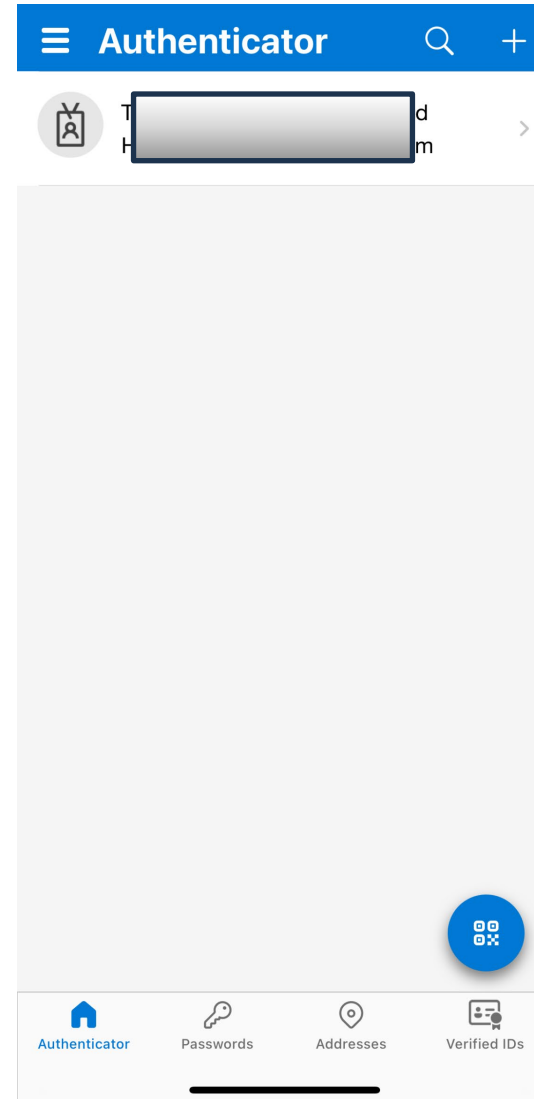
84

No numbers in your app? Make sure to upgrade to the latest version.

[I can't use my Outlook mobile app right now](#)

Step 7: Confirm and Test

- 1. Once the QR code is scanned, the account will appear in the Microsoft Authenticator app.
- 2. Test the setup by entering a verification code into the corresponding service to ensure it's working correctly.

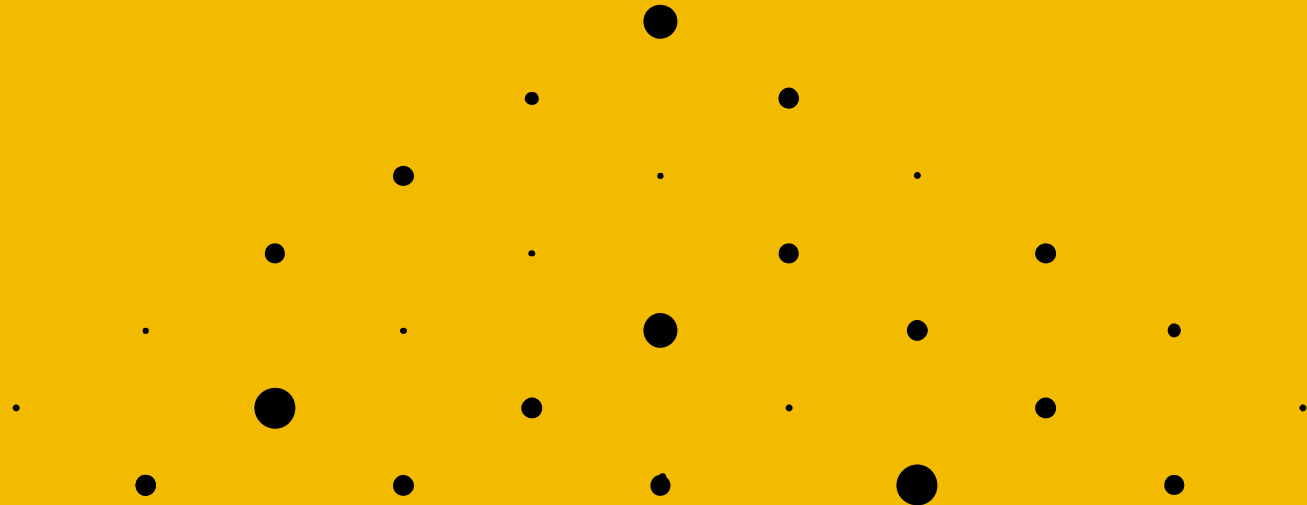


More information available:

[About Microsoft Authenticator - Microsoft Support](#)

Proximity Warning System Data

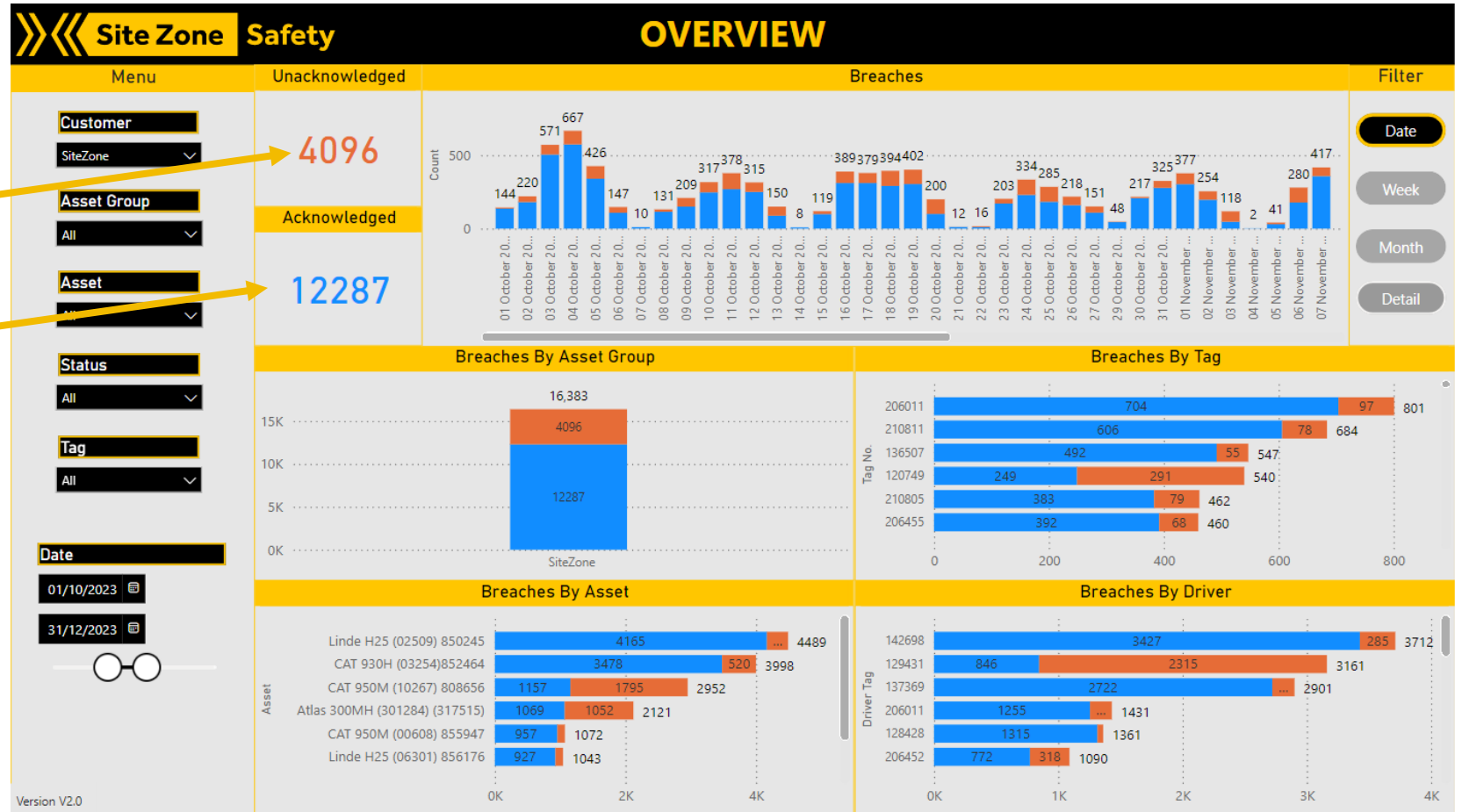
Microsoft | Power BI



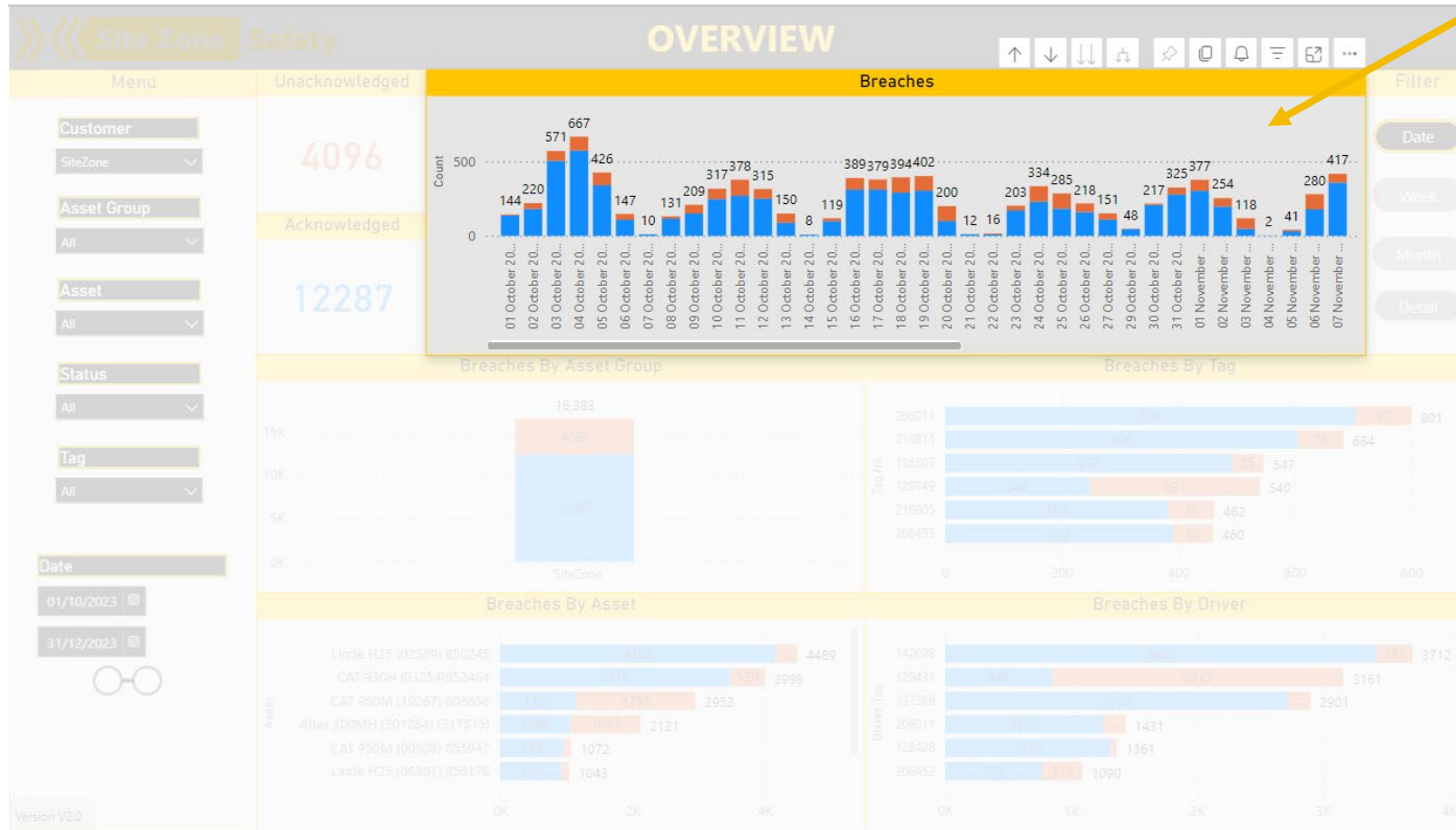
Dashboard overview

Total breaches for the selected dates

- **Unacknowledged** – the person entered the detection zone, should not have been in the detection zone, and left again.
- **Acknowledged** – the person has been acknowledged by the driver pressing the red acknowledge button on the display and allowed into the detection zone. This should only be done if correct protocol has been followed (e.g. thumbs up)
- If a machine is fitted with SmartBubble and the machine is in a safe state e.g. *deadmans handle engaged* no breach is recorded.

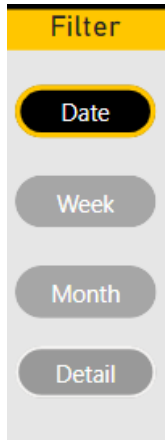


Dashboard overview

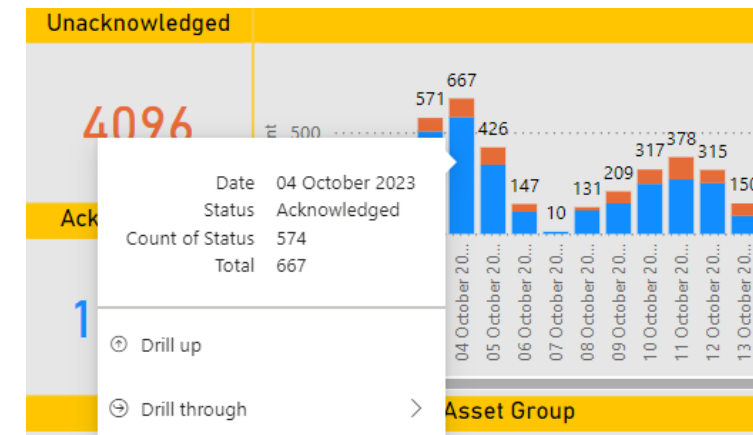


Total breaches by date, week or month

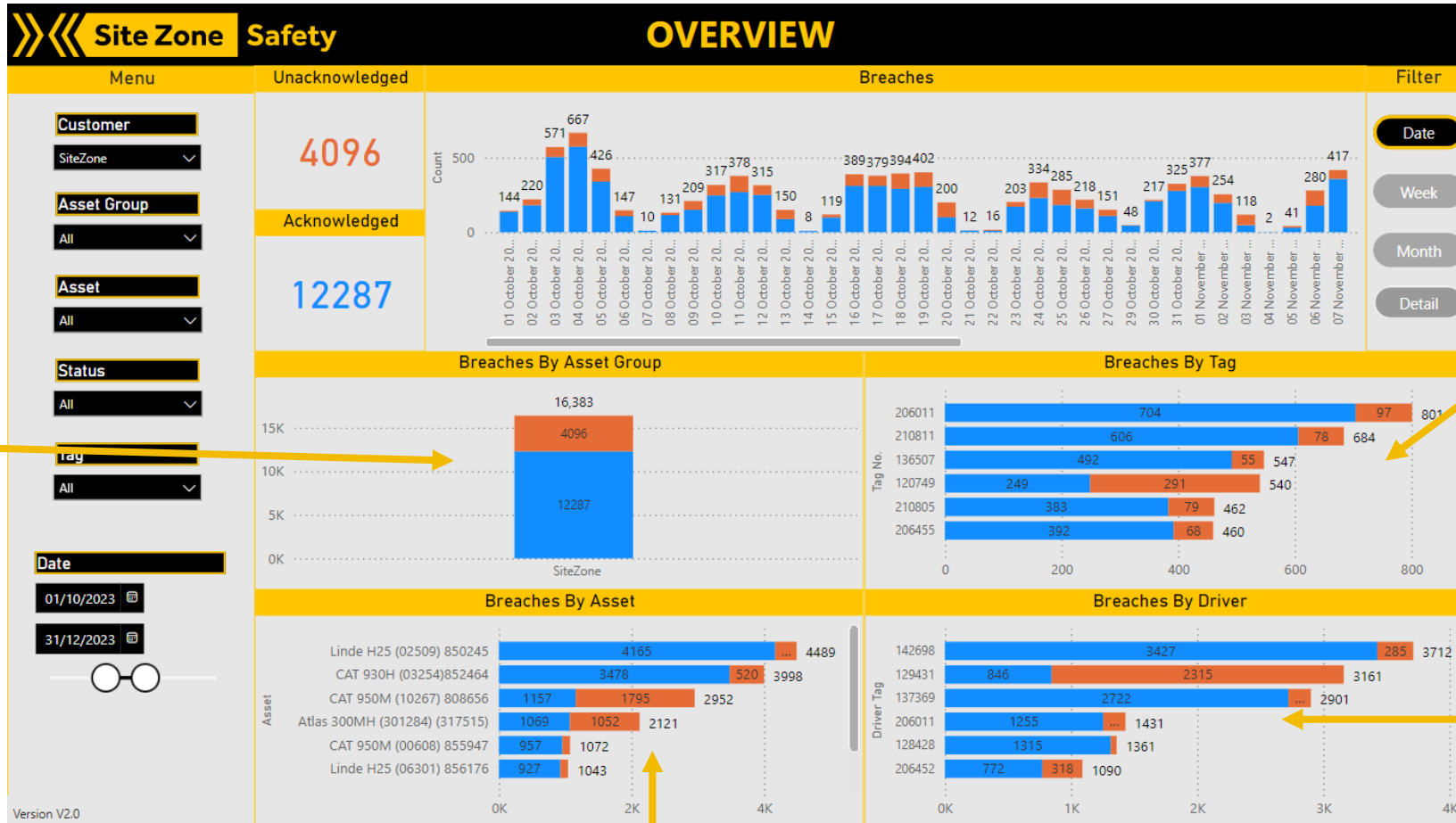
Use the filters on the right-hand side to switch between date, week and month.



Hover your mouse over the bar chart to see the totals



Dashboard overview



Breaches by site. If you have access to more than one site, you can compare them here.

Shows you the tag number that created the breach.

Breaches by machine/asset.

Shows you the driver tag that was paired when the breach occurred. If it says, 'No driver', the system hasn't been correctly paired to the driver's tag.

Menu

The screenshot shows a 'Menu' interface with the following filters:

- Customer**: SiteZone (dropdown)
- Asset Group**: All (dropdown)
- Asset**: All (dropdown)
- Status**: All (dropdown)
- Tag**: All (dropdown)
- Date**: 01/10/2023 and 31/12/2023 (date range selector with a slider and magnifying glass icon)

Version V2.0

This will be pre-set on your company.

If you have access to more than one site, you can select them here.

You can filter to only show selected vehicles.

Filter your breaches to show acknowledged or unacknowledged only.

If you want to look at breaches by a tag ID, filter here.

Select the date period you would like to view. The circles allow you to slide the date range.

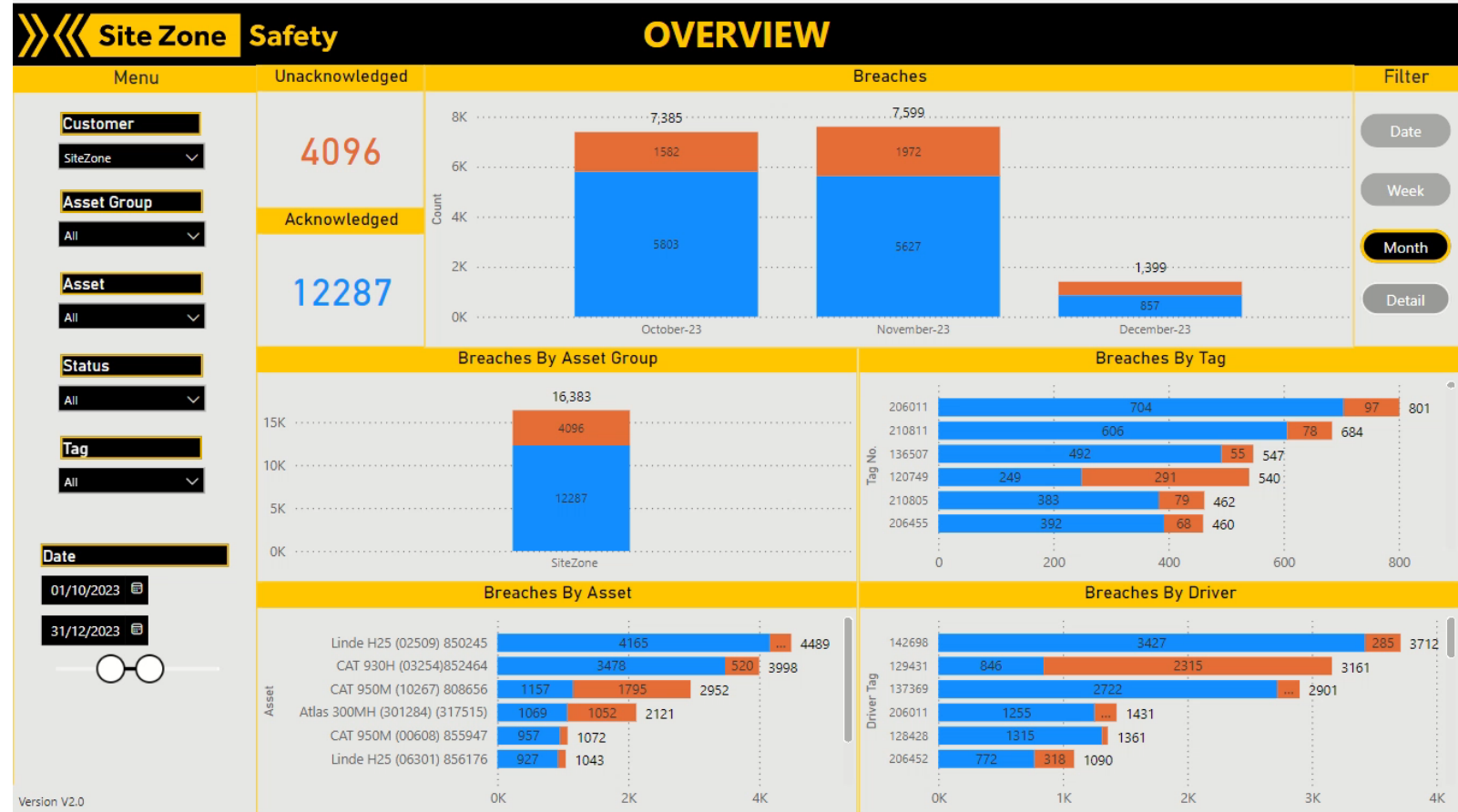
Detailed analysis

You can delve deeper into your data by selecting a single day or week. **The video on the right shows you how.**

- Using the filters on the right-hand side select **date** or **week**. This changes the bar chart.
- Click on the date or week you want to analyse
- The 'Detail' button will now be highlighted
- Click on the Detail button and you will be taken to a new detailed overview

Tip: The detail analysis won't appear when **Month** is selected.

To get back to the main screen use the 'Back to overview' button on the bottom left of the screen.



Detailed analysis

Site Zone Safety
BREACH DETAIL

Menu

customer

SiteZone

Asset Group

All

Asset

All

Status

All

Tag

All

Hour

All

[Back to Overview](#)

26 November 2023 48

Date Week No

Breaches By Day

Status ● Acknowledged ● Unacknowledged

Day	Count
Mon	200
Tue	425
Wed	703
Thu	538
Fri	203
Sat	5
Sun	101

Breaches By Hour

Hour	Count
0	10
1	19
2	1
3	17
4	24
5	7
6	6
7	93
8	336
9	159
10	364
11	280
12	230
13	186
14	96
15	121
16	17
17	1
18	5
19	1
20	8
21	8
22	1

Breaches By Tag

Tag No.	Breaches
136507	196
206011	99
203237	44, 32
206455	62
133434	53
120749	47
210807	38
120531	58
134200	44
136457	44

Breaches By Driver

Driver Tag	Breaches
142698	562
137369	365
128428	377
129431	178
206011	119
206452	119
213337	96
206453	55
134048	39
142834	25

This shows you the date/week you are viewing.

See your breaches for each day that week.

This chart shows cumulatively which hours of the day get most breaches for the whole week.

Scroll all data for the time. Can be sorted by clicking on the top of each column.

Shows you the tag number that created the breach.

Shows you the driver tag that was paired when the breach occurred.

Drilling into the data

The dashboard is interactive.

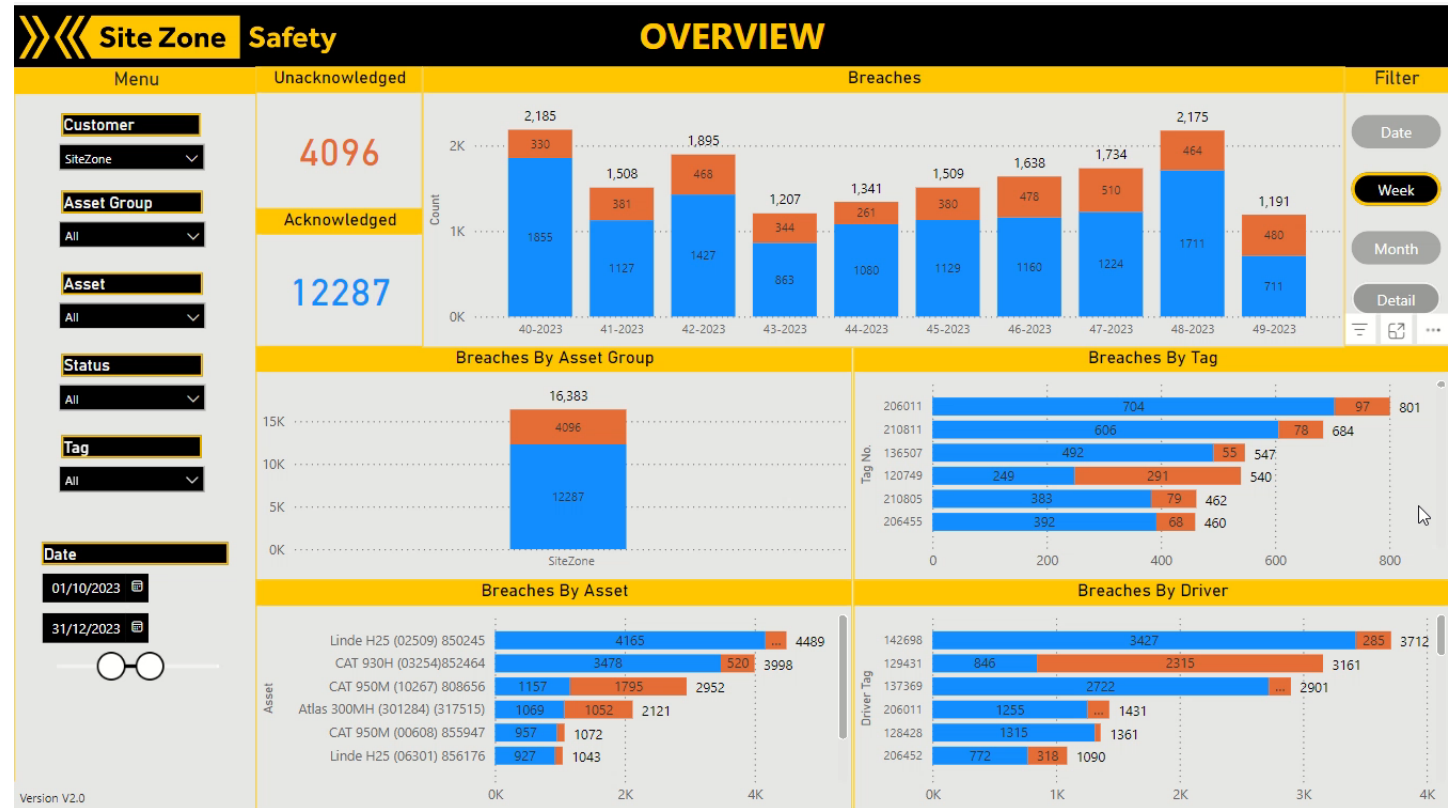
By clicking on any bar chart or axis label, you can highlight specific data points to gain greater insights.

The video on the right shows how you select the 'Unacknowledged' alerts for a specific machine. This greys out the remaining data to show you:

- tag numbers unacknowledged
- the days when unacknowledged breaches occurred
- the driver tag number

To clear your selection, click anywhere on the dashboard that isn't a bar chart.

Tip: You can use this to discuss breaches with a specific tag wearer or machine operator to understand why it happened and improve performance.



Options on each data set/section

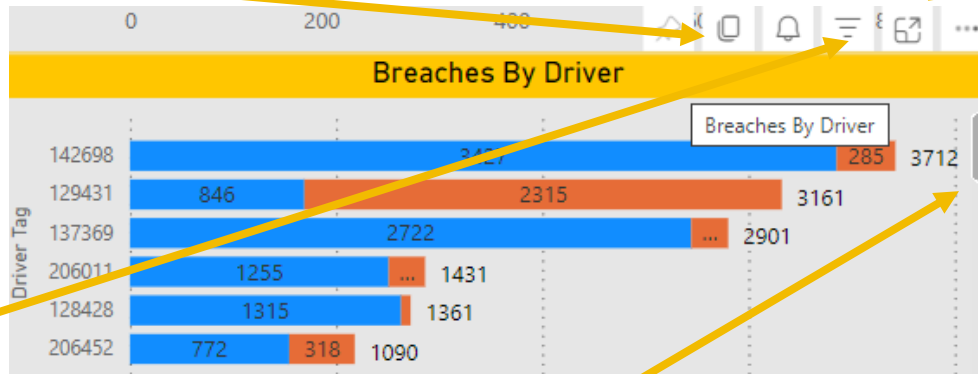
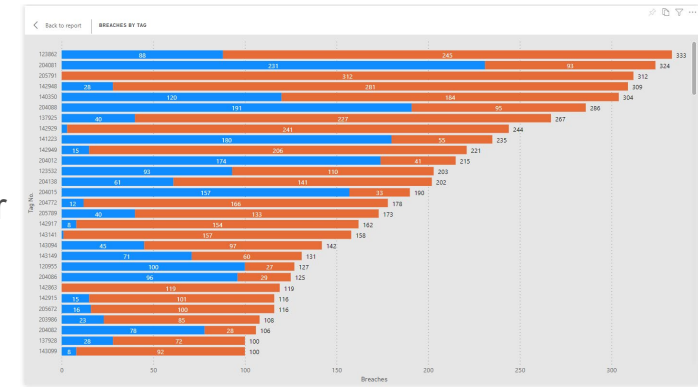
Use the additional menu buttons (top right of each section), for more options. *Note: These buttons only show when your mouse hovers over the dashboard section and the buttons are associated to the section of the dashboard directly below it.*

Copy – you can copy the image if you want to use it in another place (e.g. report or email).

Focus – the focus button opens a specific data set to enable a larger view and analysis.

Filter – shows you what the current filter is set to.

Scroll bar - If there is a lot of data e.g. tags or assets (machines) you will get a scroll bar on the righthand side to enable you to scroll up and down.



- Share
- Set alert
- Add a comment
- Export data
- Show as a table
- Spotlight
- Get insights
- Sort axis
- Sort legend

Exporting data

All dashboard charts can be copied, printed, embedded, or exported as Excel, PDF or PowerPoint documents for offline review and distribution.

To export the full report, select the export button at the top of the dashboard.

The screenshot shows the Site Zone Safety dashboard interface. At the top, there is a navigation bar with 'File', 'Export', 'Share', 'Chat in Teams', 'Get insights', and 'Set alert'. The 'Export' menu is open, showing options for 'Analyze in Excel', 'PowerPoint', and 'PDF'. The dashboard content includes a sidebar with filters for 'SiteZone', 'Asset Group', 'Asset', 'Status', 'Tag', and 'Date'. The main area features a large 'OVERVIEW' section with a 'Count' of 12287 and a bar chart showing 'Breaches By Asset Group' for the periods 40-2023, 41-2023, 42-2023, and 43-2023. The bar chart data is as follows:

Period	Count
40-2023	2,185
41-2023	1,508
42-2023	1,895
43-2023	1,207

The 'Breaches By Asset Group' chart shows a total count of 16,383, with 4,096 breaches attributed to SiteZone.

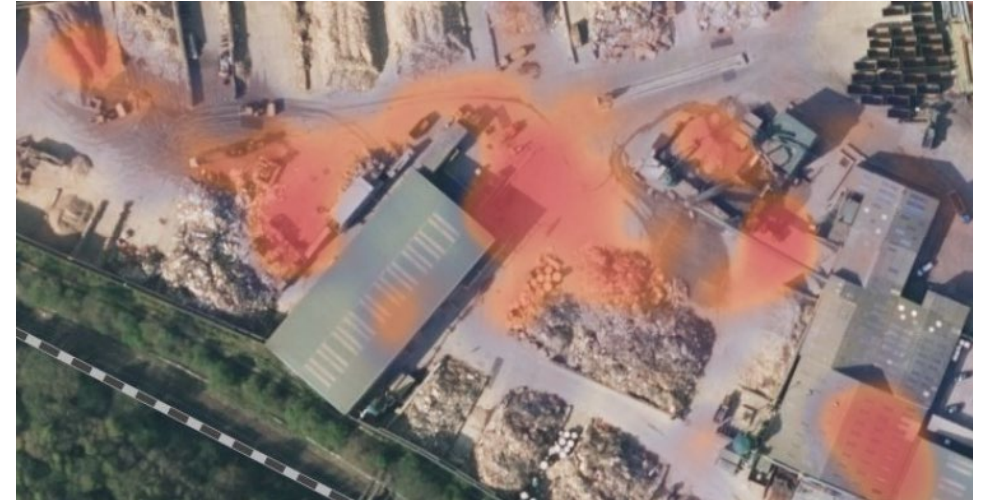
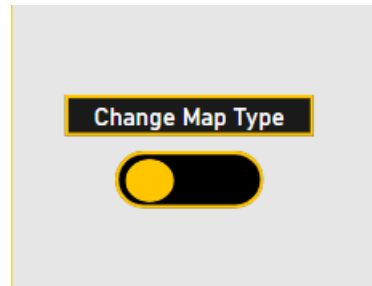
Heat maps

Discover the hot spots for zone breaches on your site

Filter by type of alert (authorised or ignored), and machine.

Toggle between map types at the bottom of the menu.

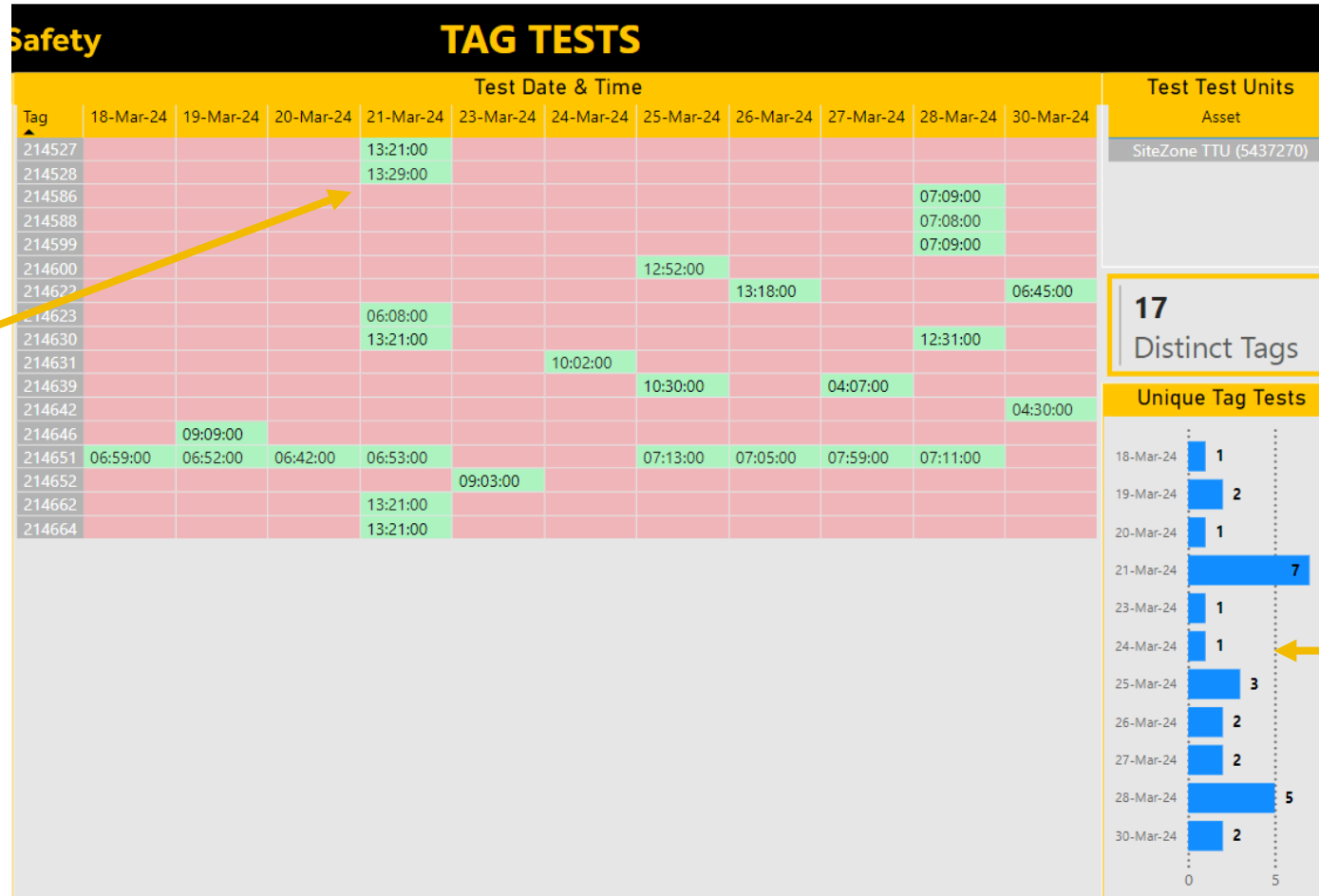
The larger the orange circle, the more zone breaches in that area. Hover over the circle for more info



**Please note: Heat maps aren't available for some users.*

Tag tests

The chart shows the last tag test time for that tag each day. If the square is red, the tag wasn't tested that day.



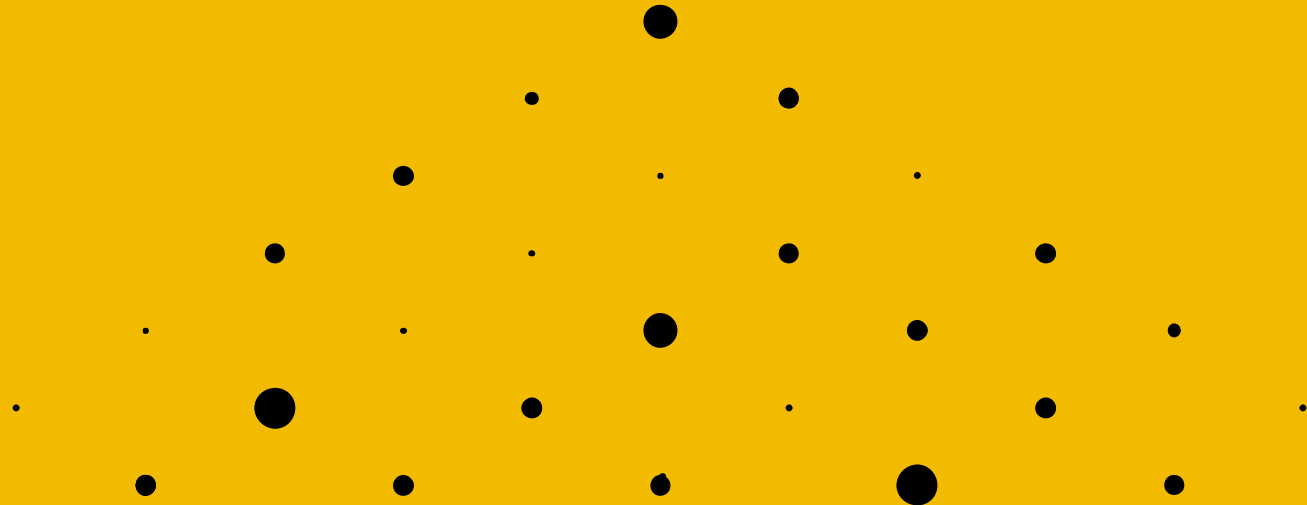
Distinct tags – this shows the total number of **unique tag tests** for the selected period.

The bar chart shows the number of unique tag tests per day. Use this as a quick count to see if it matches the number of employees working that day and know if everyone is testing their tag.

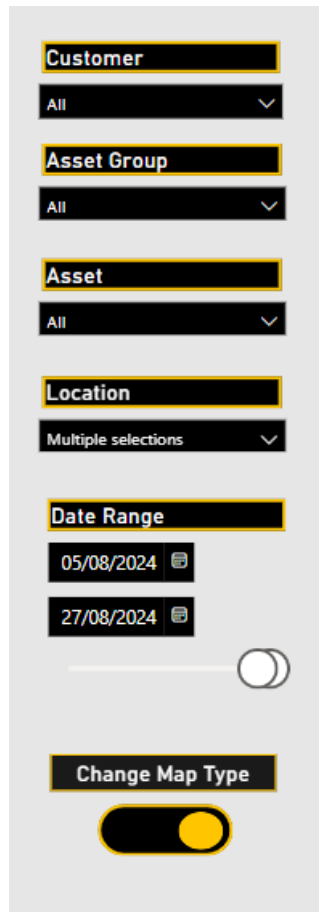
**This is an optional extra that may not have been included as part of your original installation.*

RCV Smart Loader Data

 Microsoft | Power BI



Menu



This will be pre-set on your company.

If you have access to more than one site, you can select them here.

You can filter to only show selected vehicles.

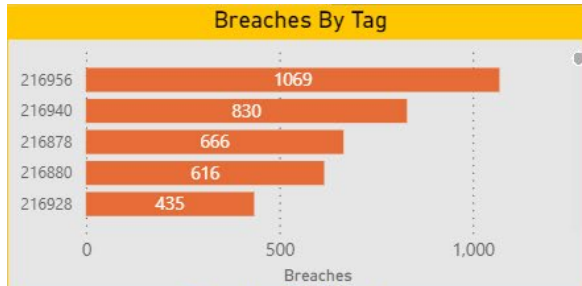
Filter your breaches by location.

Select the date period you would like to view. The circles allow you to slide the date range.

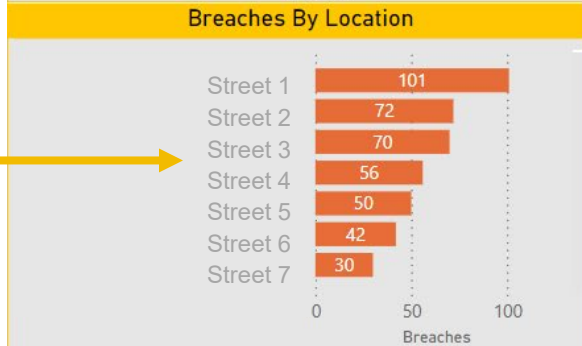
Toggle between map types.

Dashboard overview

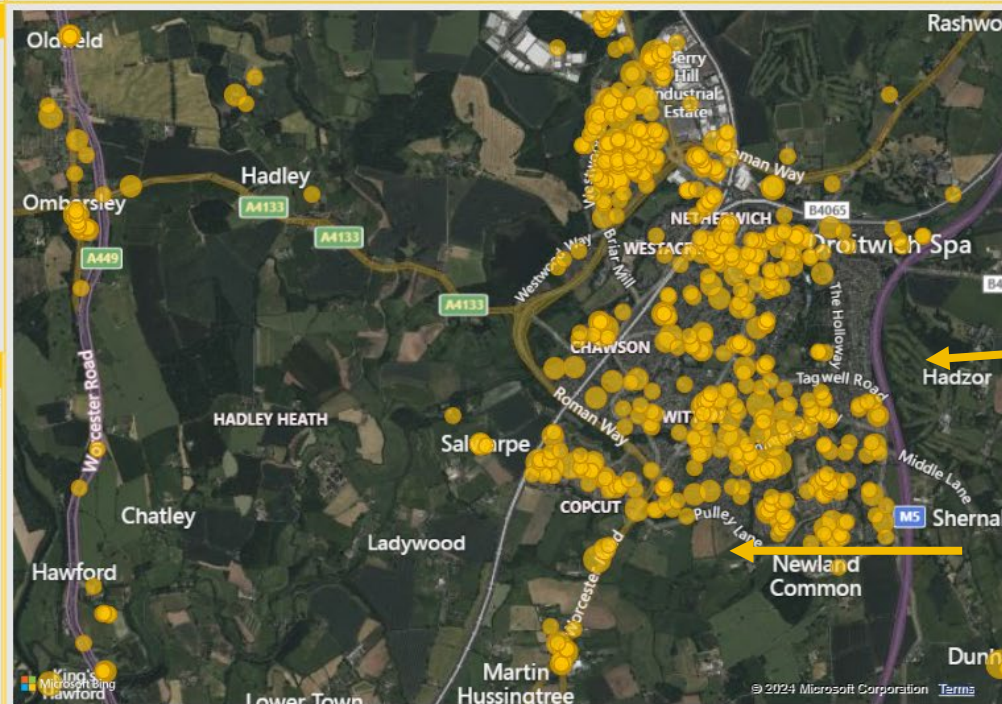
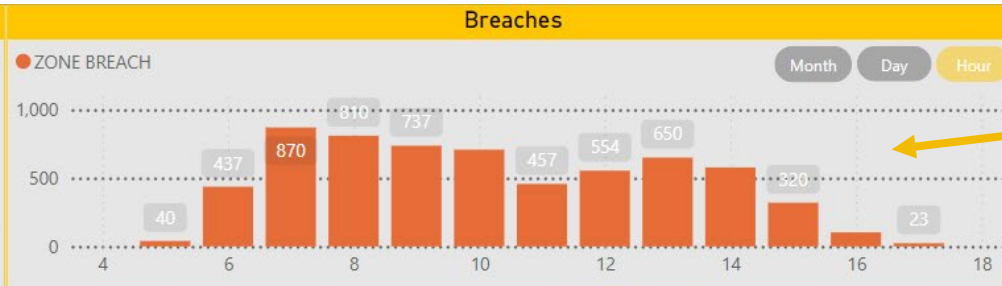
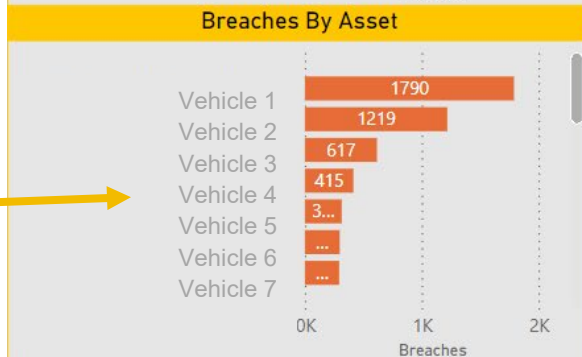
Shows you the tag number that created the danger zone breach.



Breaches by street. We recommend filtering out your depot in the menu.



Breaches by Vehicle.



Total breaches by hour, day, or month (Cumulative for the period of time selected)

Use the filters on the top to switch between hour, day, and month.

Discover the hot spots on your rounds for zone breaches.

The larger the orange circle, the more zone breaches in that area. Hover over the circle for more info.

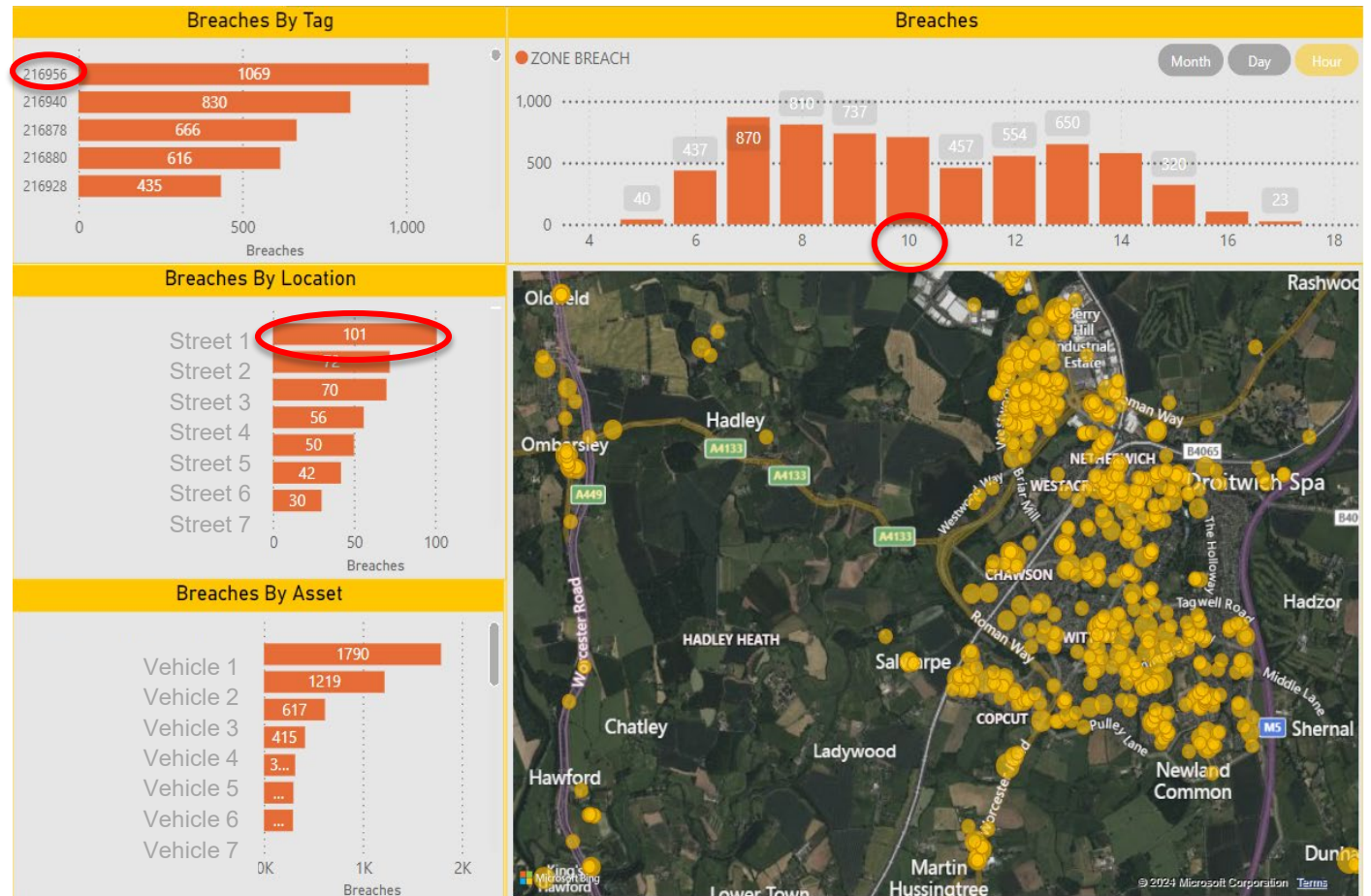
Drilling into the data

The dashboard is interactive.

By clicking on any bar chart or axis label, you can highlight specific data points to gain greater insights.

To clear your selection, click anywhere on the dashboard that isn't a bar chart.

Tip: You can use this to discuss breaches with a specific tag wearer or vehicle crew to understand why it happened and improve performance.



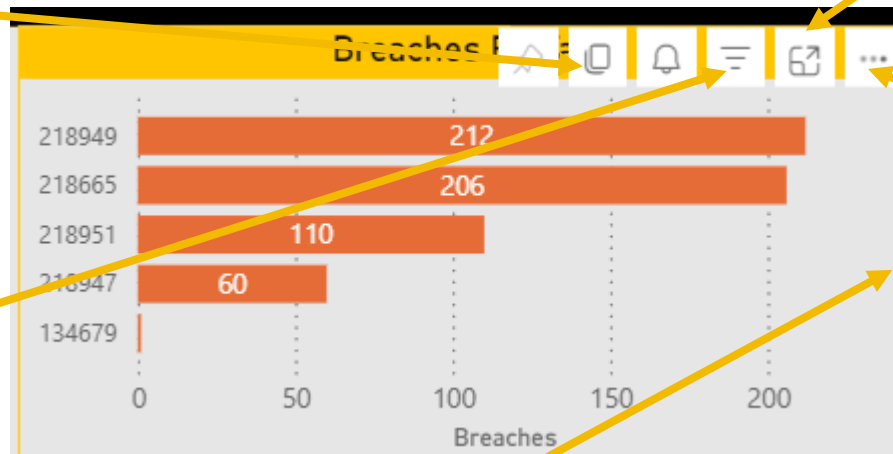
Options on each data set/section

Use the additional menu buttons (top right of each section), for more options. *Note: These buttons only show when your mouse hovers over the dashboard section and the buttons are associated to the section of the dashboard directly below it.*

Copy – you can copy the image if you want to use it in another place (e.g. report or email).

Focus – the focus button opens a specific data set to enable a larger view and analysis.

Filter – shows you what the current filter is set to.



More options – enables you to change the view, comment with colleagues, and export in Excel.

- Share
- Set alert
- Add a comment
- Export data
- Show as a table
- Spotlight
- Get insights
- Sort axis
- Sort legend

Scroll bar - If there is a lot of data e.g. tags or assets (machines) you will get a scroll bar on the righthand side to enable you to scroll up and down.

Exporting data

All dashboard charts can be copied, printed, embedded, or exported as Excel, PDF or PowerPoint documents for offline review and distribution.

To export the full report, select the export button at the top of the dashboard.

