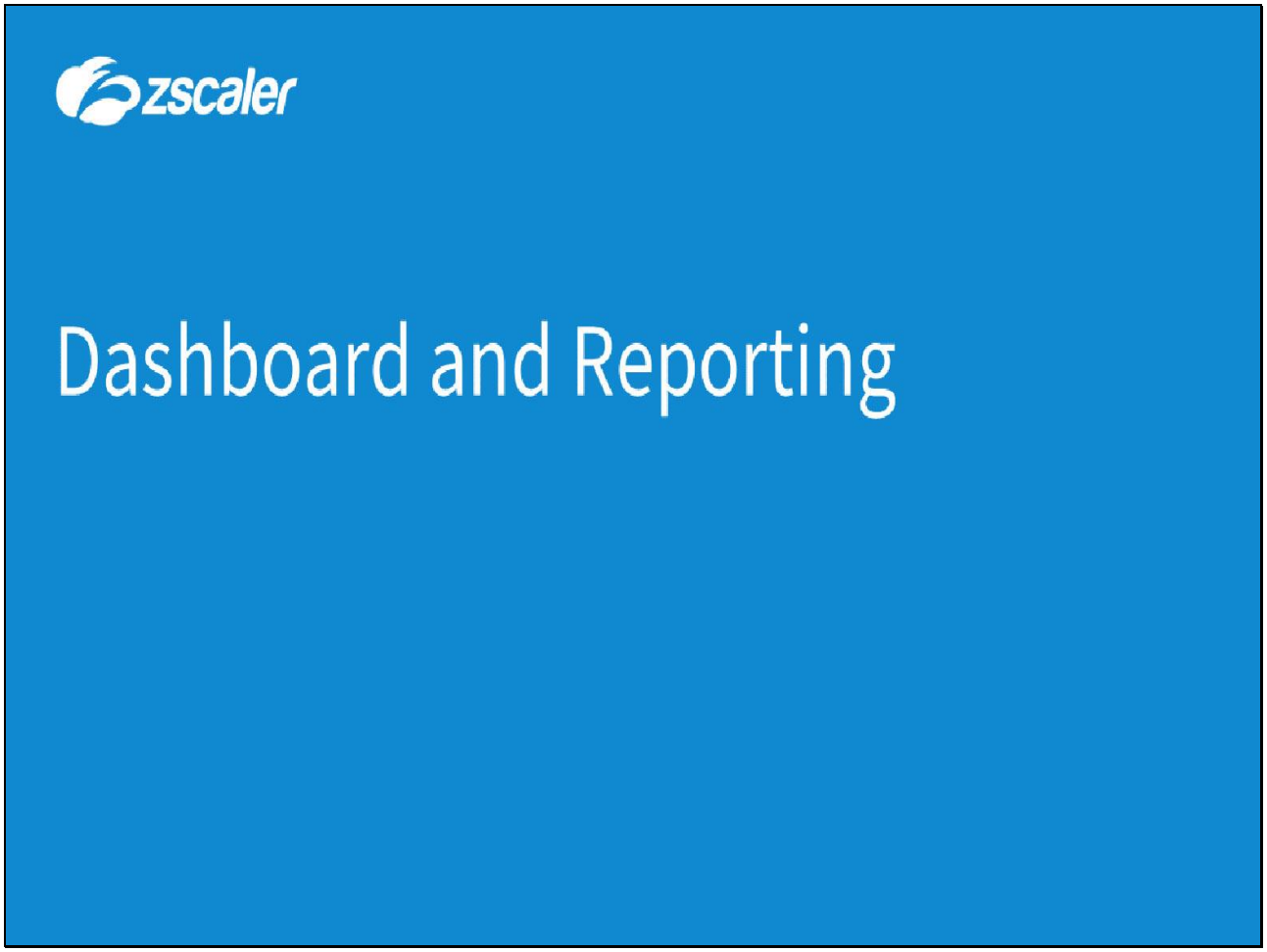
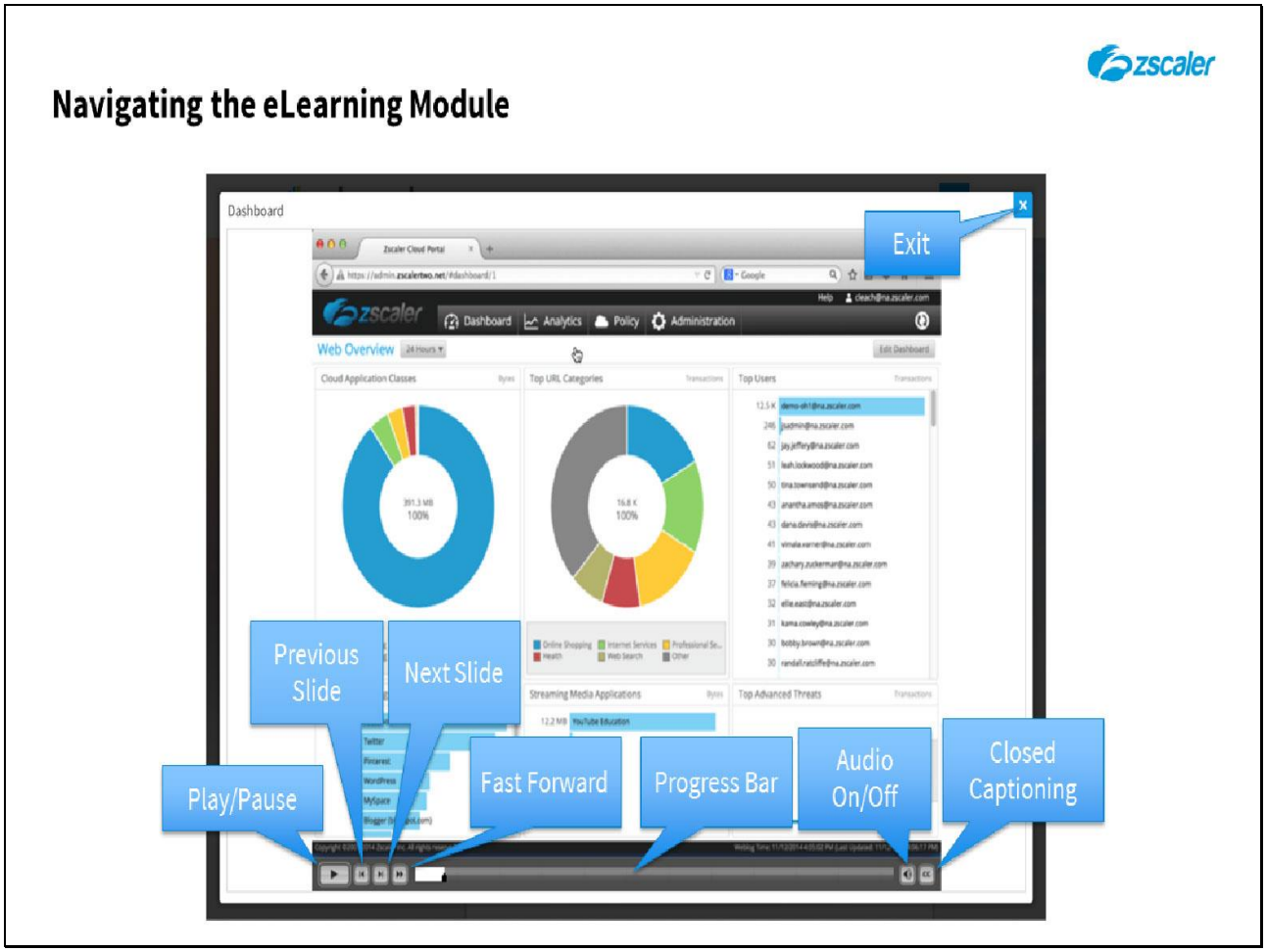
Slide 1 - Dashboard and Reporting



Slide notes

Hello and Welcome to the ZCCA eLearning module for the Admin UI Dashboard and Reporting.

Slide 2 - Navigating the eLearning Module



Slide notes

Here is a quick guide to navigating this eLearning module. There are various controls for playback including Play/Pause, Previous and Next Slide, and Fast Forward. You can also mute the Audio or enable Closed Captioning which will cause a transcript of the module to be displayed on the screen. Finally, you can click the “X” button if you wish to exit.

Slide 3 - Module Agenda

Slide notes

During this module we will cover editing Dashboards, review system defined reports, and using the Dashboard and reporting to track and resolve issues.

Slide 4 - Editing Dashboards

Slide notes

Let’s begin with an overview of the dashboards and how to edit them to suit each admins preferences.

Slide 5 - Slide 5

Slide notes

When you log into the Zscaler Admin UI you are presented with the Dashboard view. This view gives you a graphical overview of your traffic flowing through the Zscaler Cloud.

Slide 6 - Slide 6

Slide notes

Multiple Dashboards are available, depending on which subscriptions you have purchased.

By default, the system will show the last 24 hours of data. You can change that by clicking the drop down and selecting a different time period.

As you move around the screen you'll notice if you hover over an item it will give you additional details and ask you to click for more information.

When you click you get the option to View Logs or Analyze Chart.

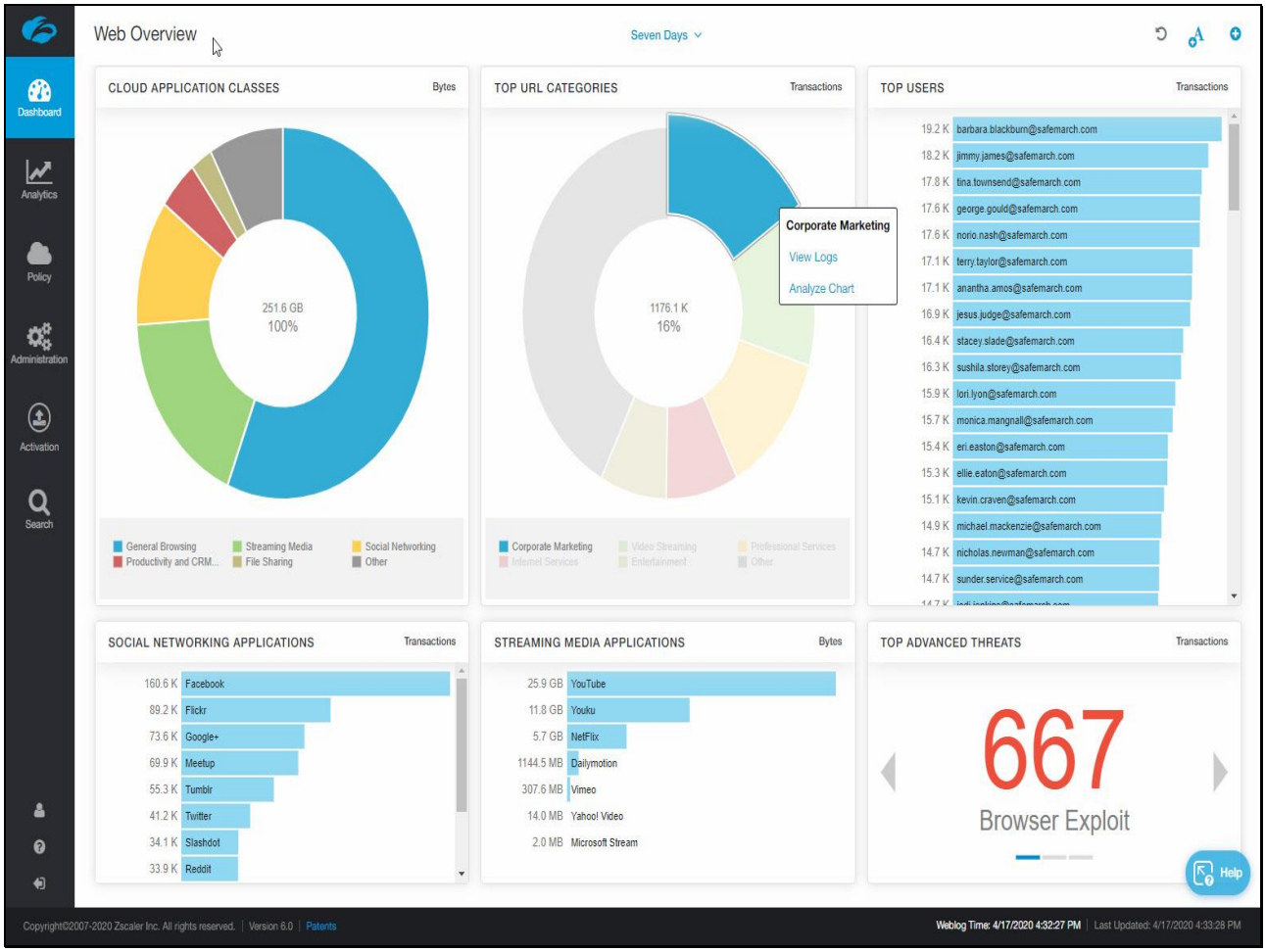
Slide 7 - Slide 7

Slide notes

If you would like to modify the dashboard and widgets to better suit your needs, you can edit them. All of the dashboards and any of the widgets may be customized. Changes to the dashboard are Admin specific so changes you make to your own admin account are not seen by other admins.

The following items can be edited: dashboard title, widget position, widget details, and can add or delete widgets.

Slide 8 - Slide 8

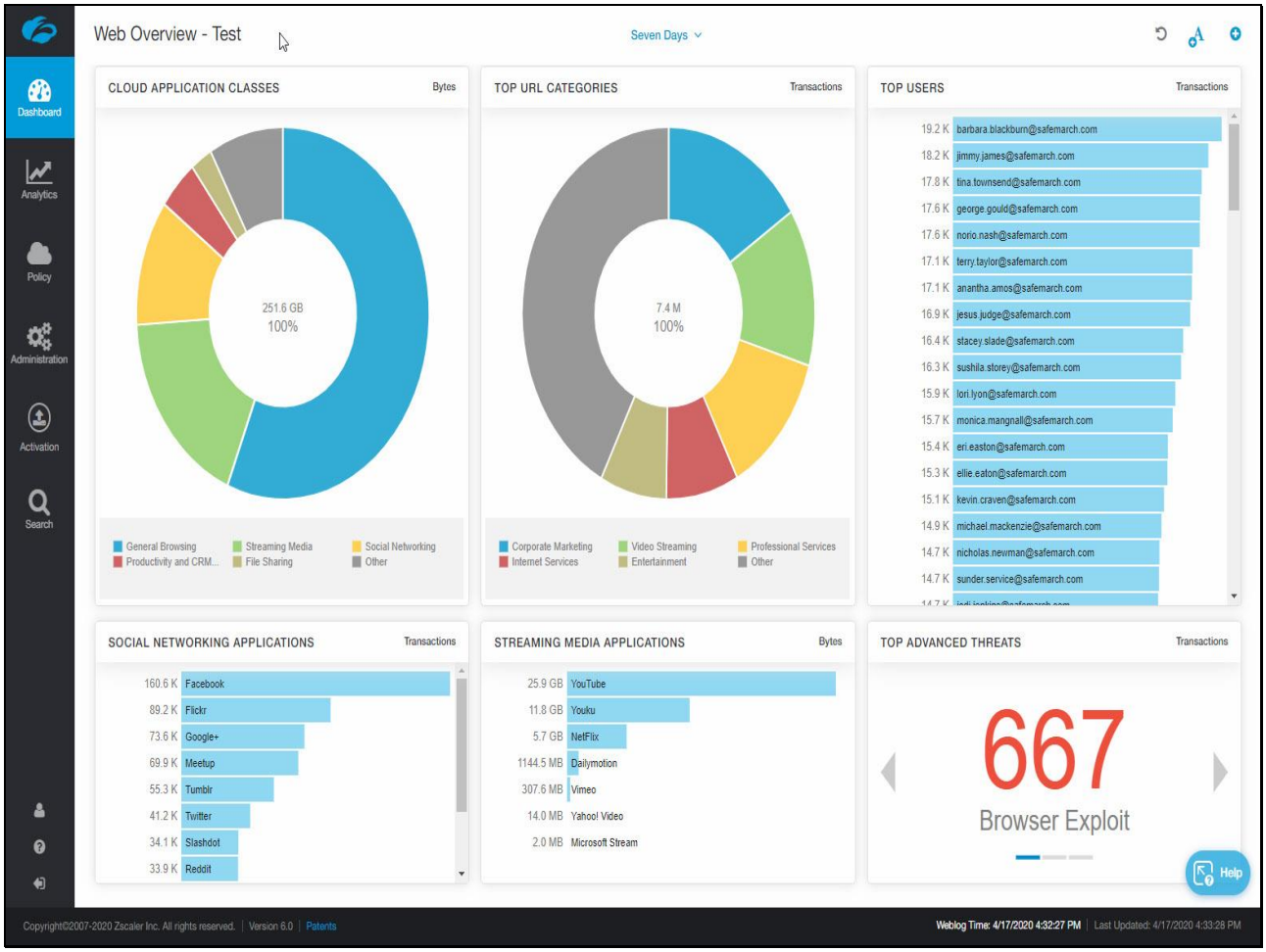


Slide notes

The title of the dashboard may also be changed if desired. To change a dashboard name simply click on the name and make the desired changes.

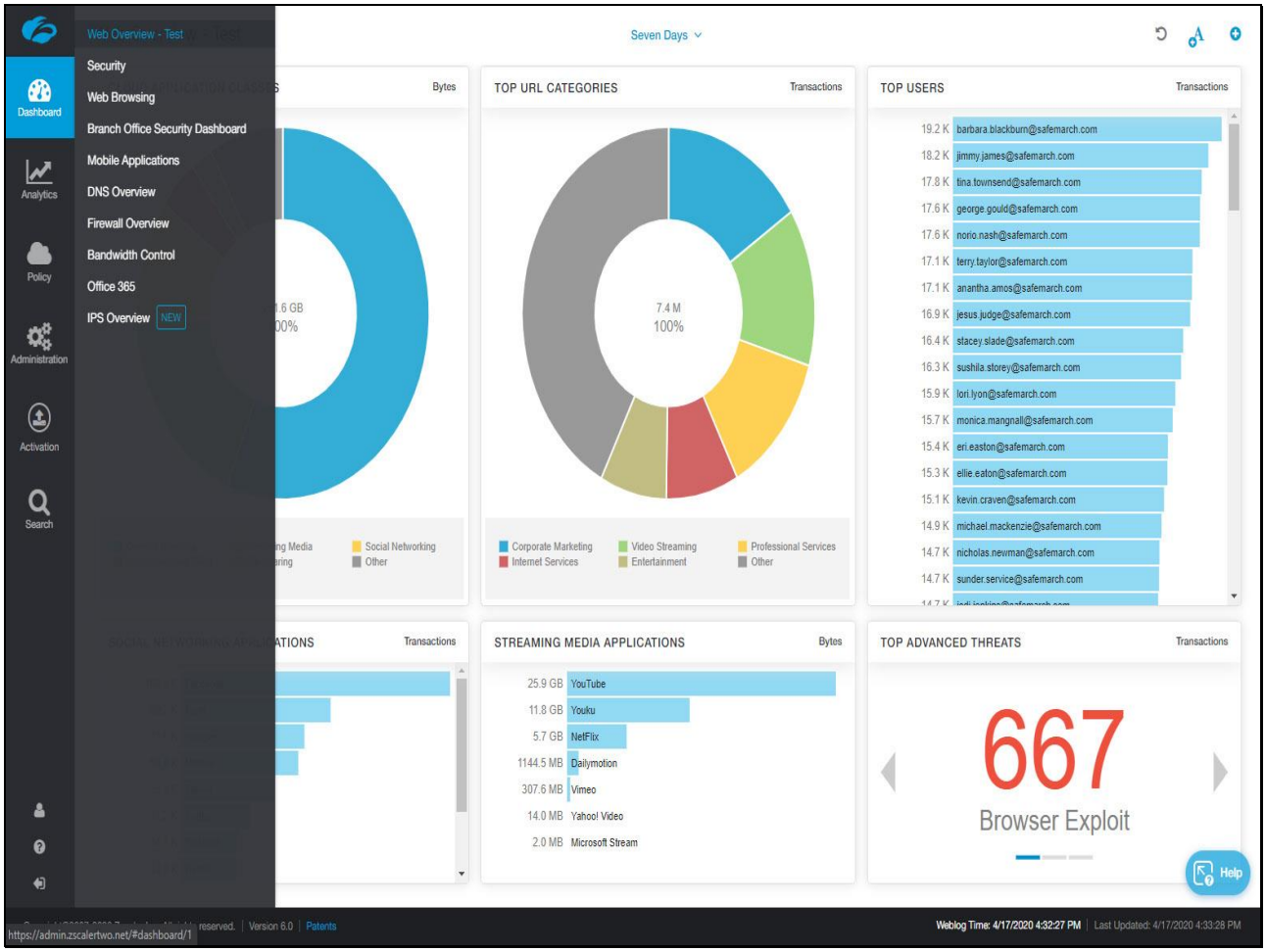
Once the dashboard name has been changed you will notice that it has also been changed in the drop-down menu of the Admin UI.

Slide 9 - Slide 9



Slide notes

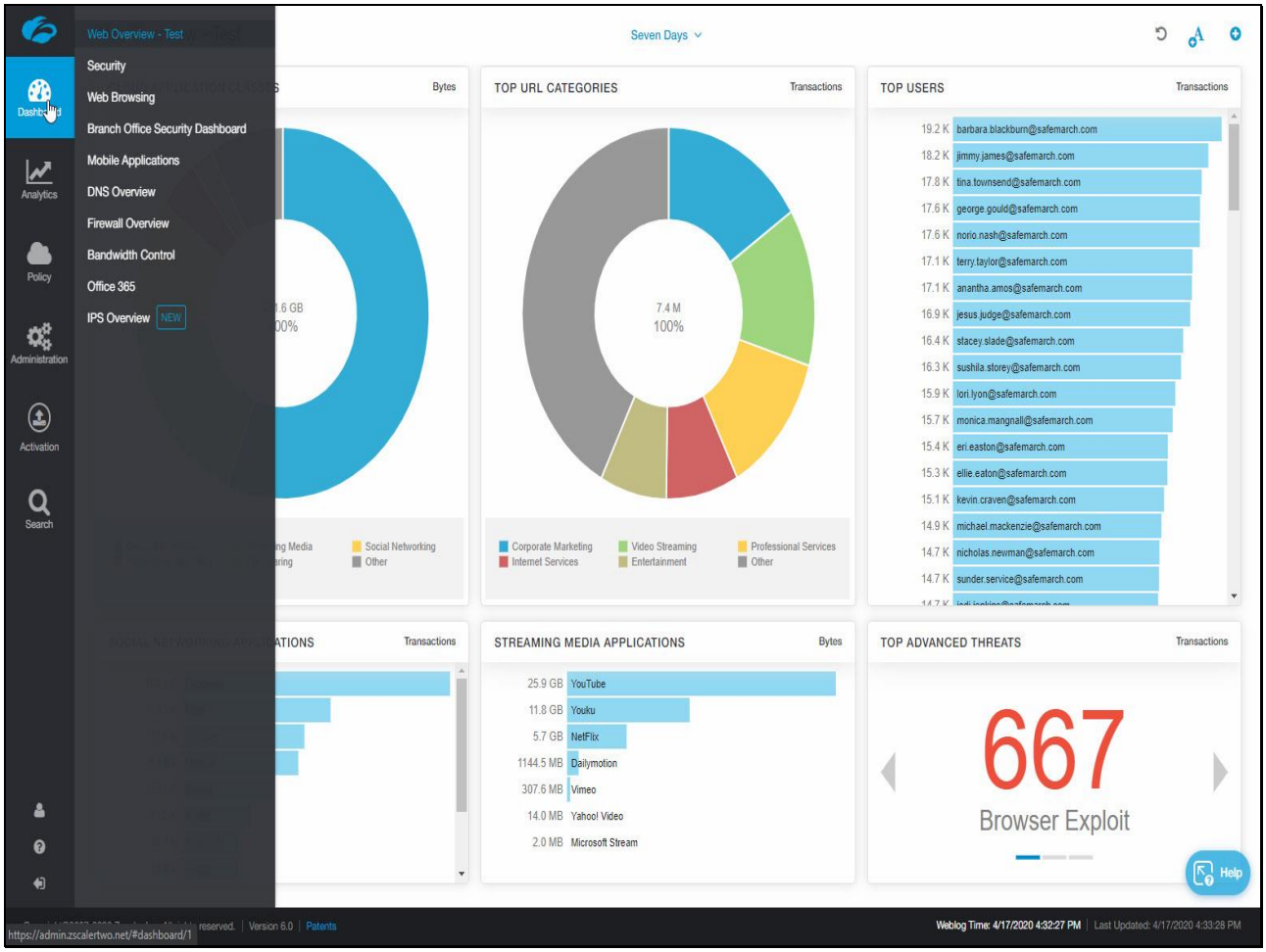
Slide 10 - Slide 10



Slide notes

To re-arrange widgets on the screen simply move your mouse over the title bar of the widget you wish to move. You will see crosshairs appear indicating that you can move the object.

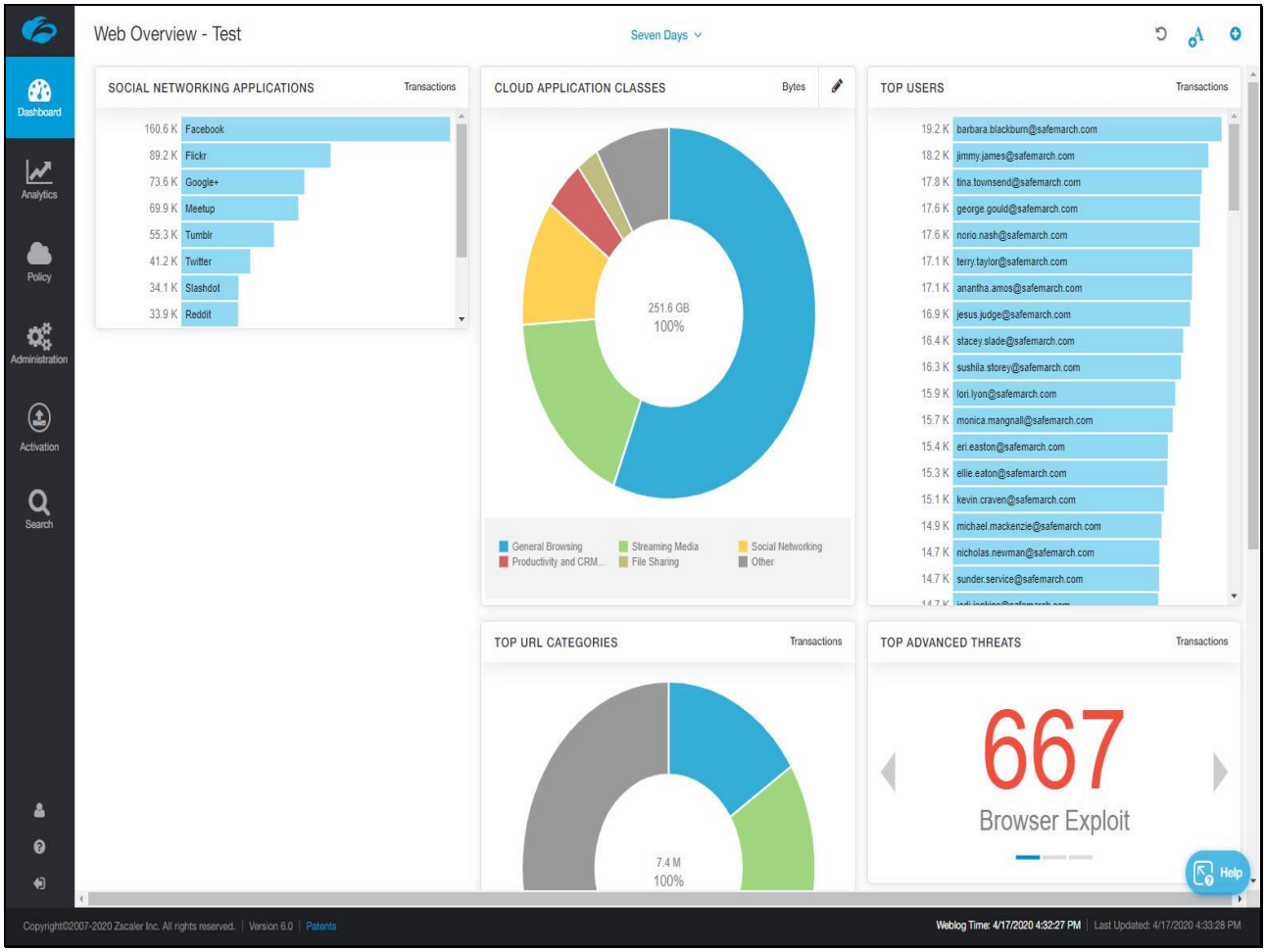
Slide 11 - Slide 11



Slide notes

Click and hold your mouse then move the widget to the desired location then release your mouse button.

Slide 12 - Slide 12

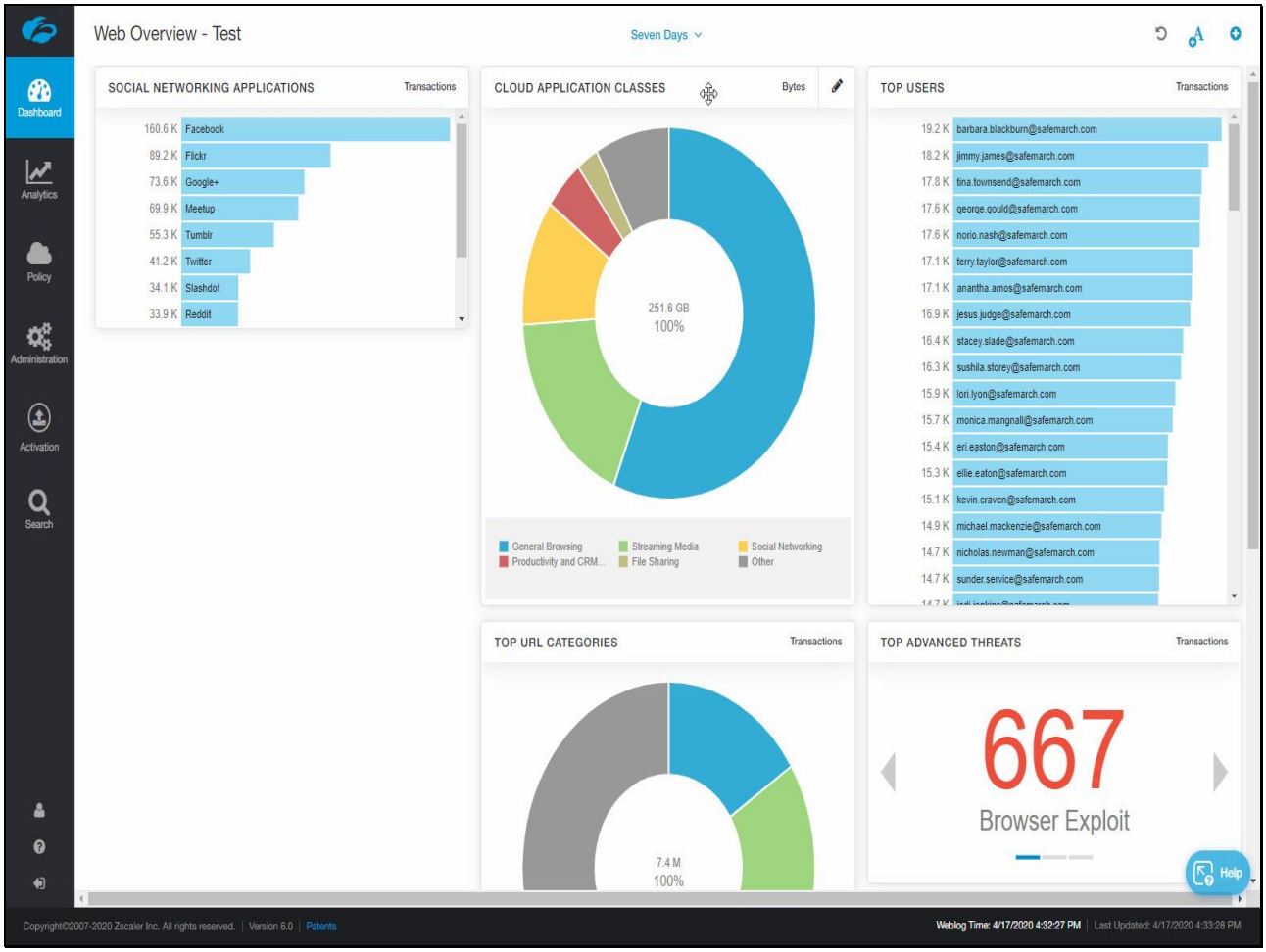


Slide notes

Notice that the Admin UI automatically re-arranges the other widgets to make room for the new widget position.

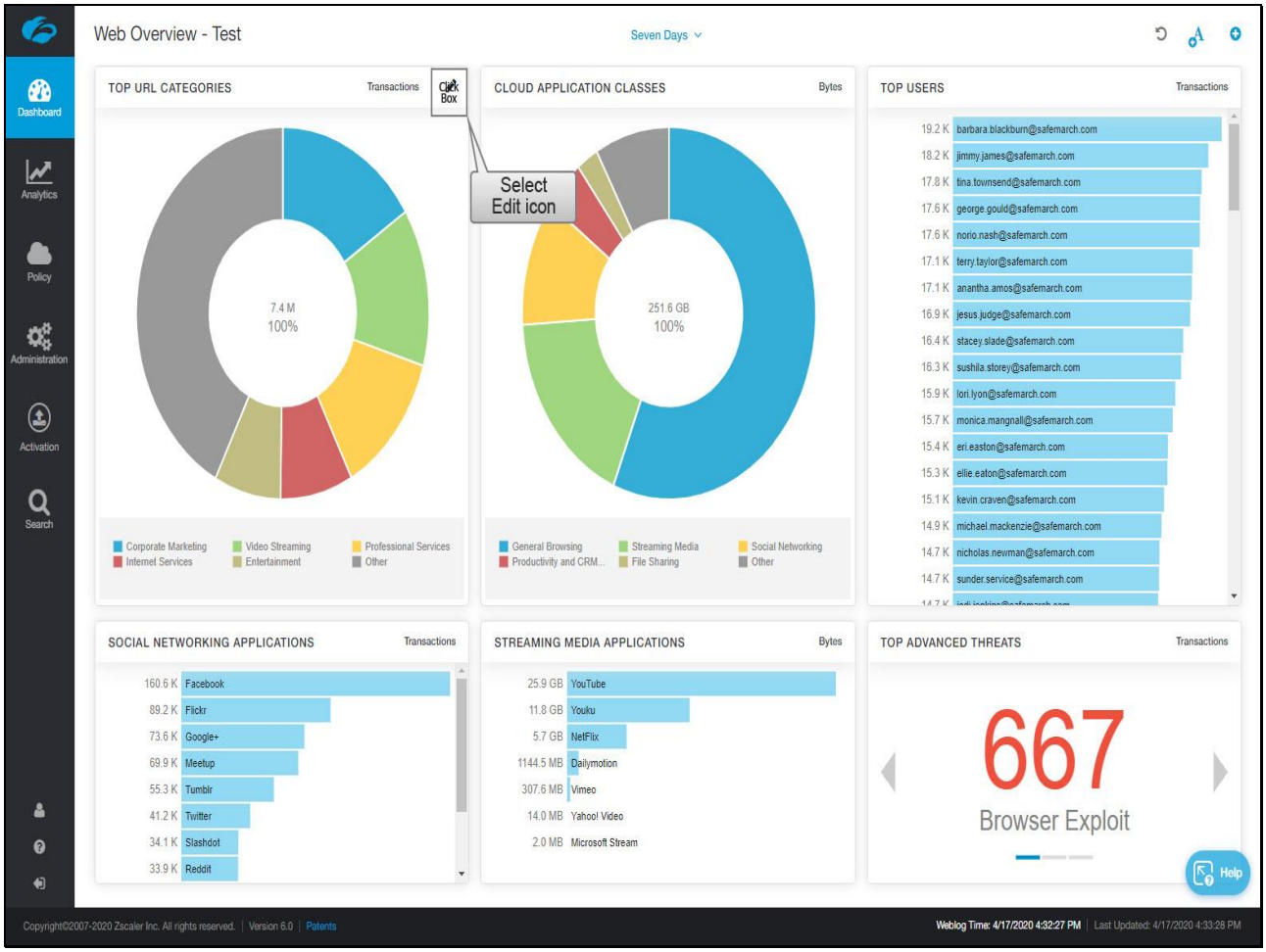
You may find that you need to fine tune the final widget placement.

Slide 13 - Slide 13



Slide notes

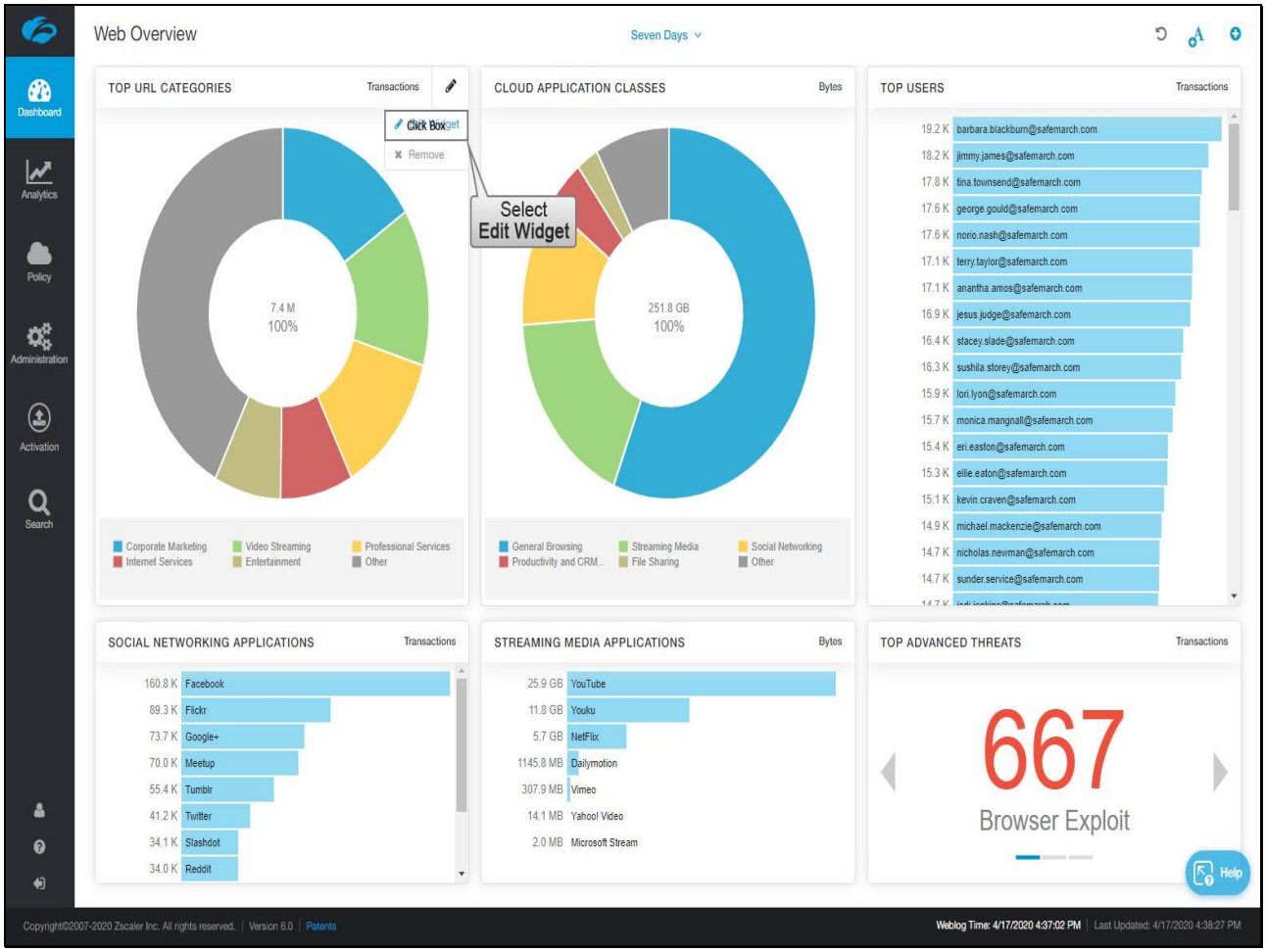
Slide 14 - Slide 14



Slide notes

Any widget can be modified or deleted. New widgets can be added as well. To delete a widget hover over the title bar to display then click the edit icon. You will see options to edit the widget or remove it. If you click remove you will be provided a warning before it is deleted.

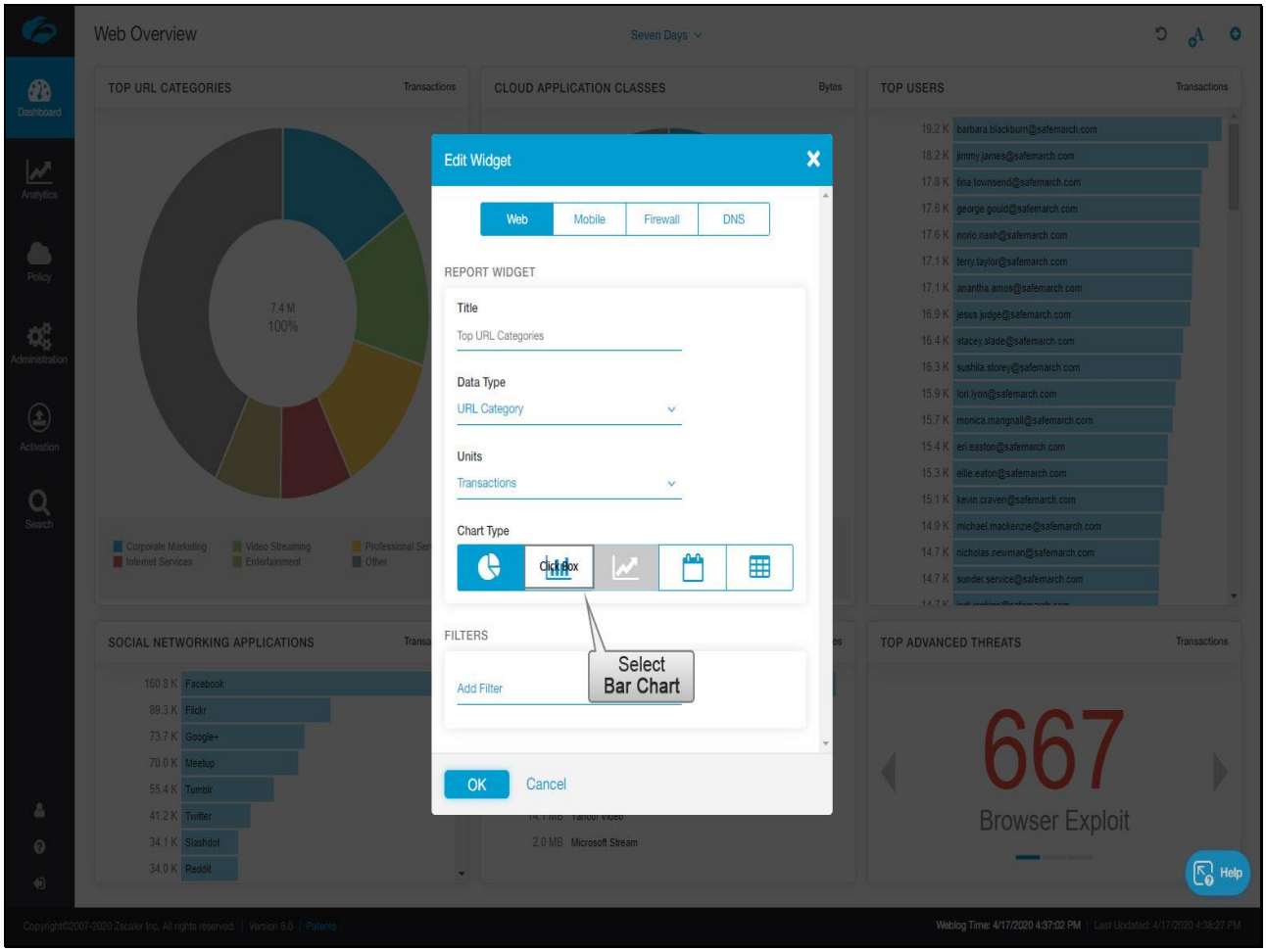
Slide 15 - Slide 15



Slide notes

Click “Edit Widget”.

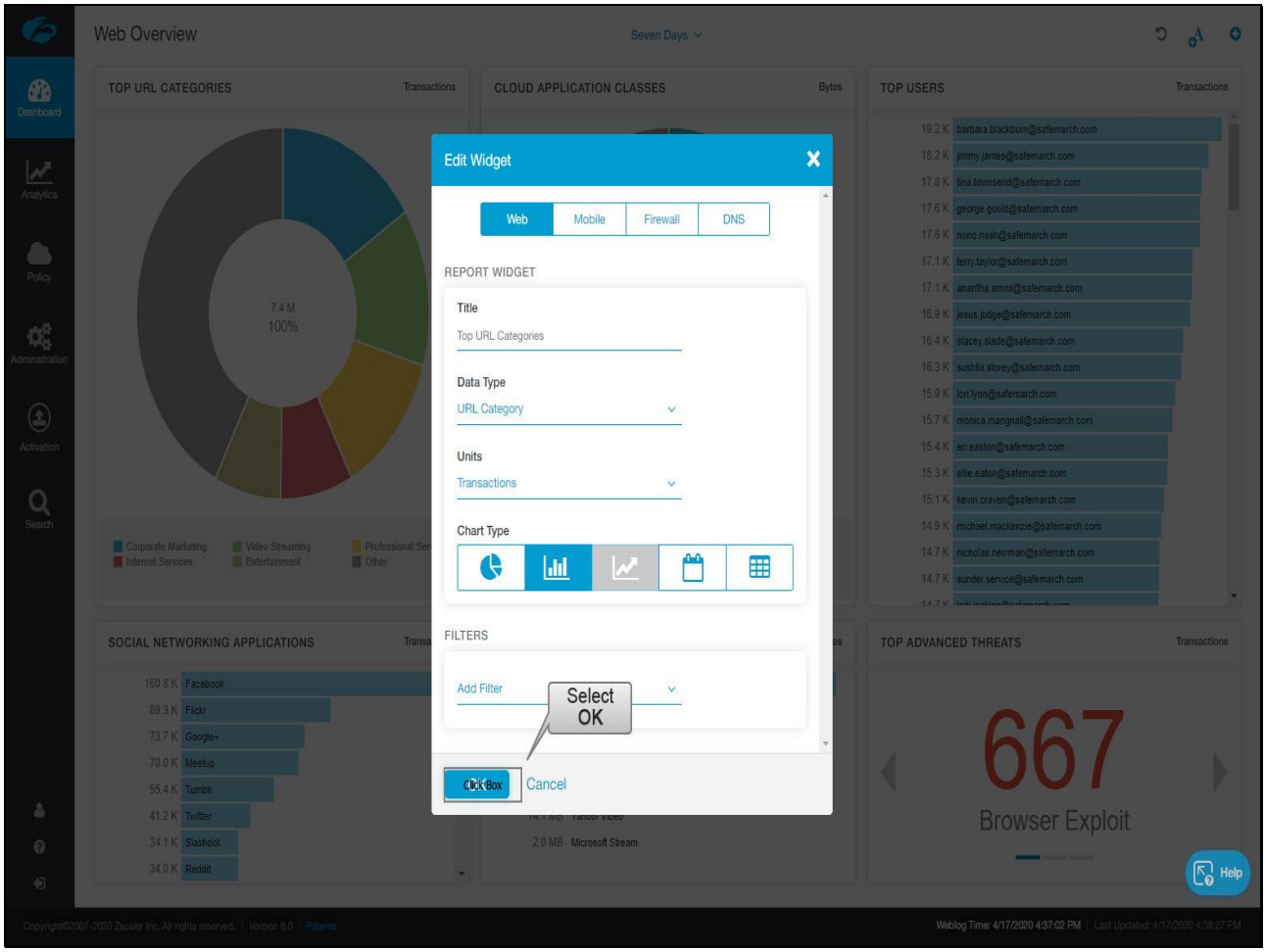
Slide 16 - Slide 16



Slide notes

Let's modify this chart to be a bar chart rather than a pie chart. Click the **Bar Chart** icon

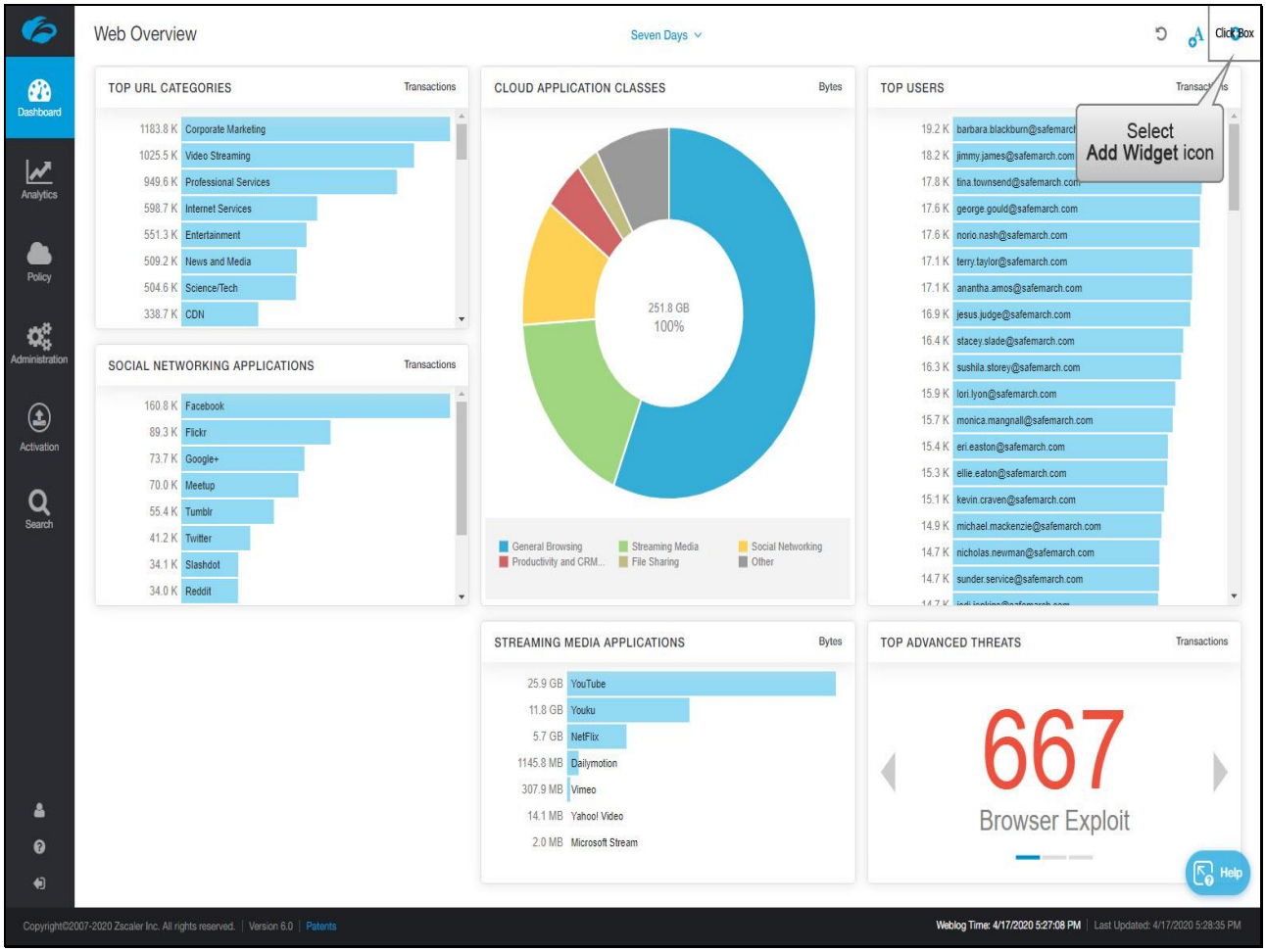
Slide 17 - Slide 17



Slide notes

Then click “**OK**”.

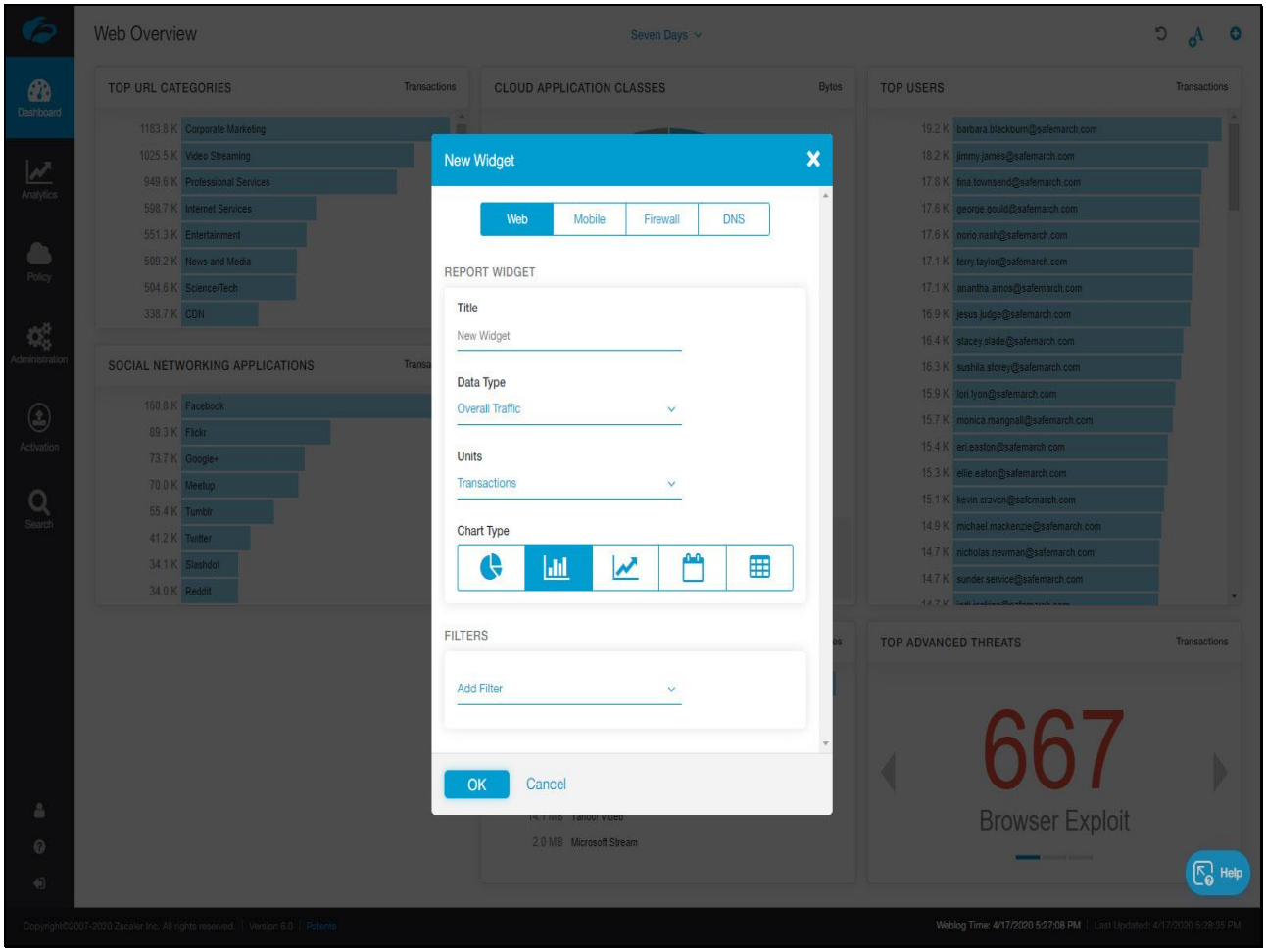
Slide 18 - Slide 18



Slide notes

A new widget can be added by clicking on the "**Add Widget**" icon in the upper right corner.

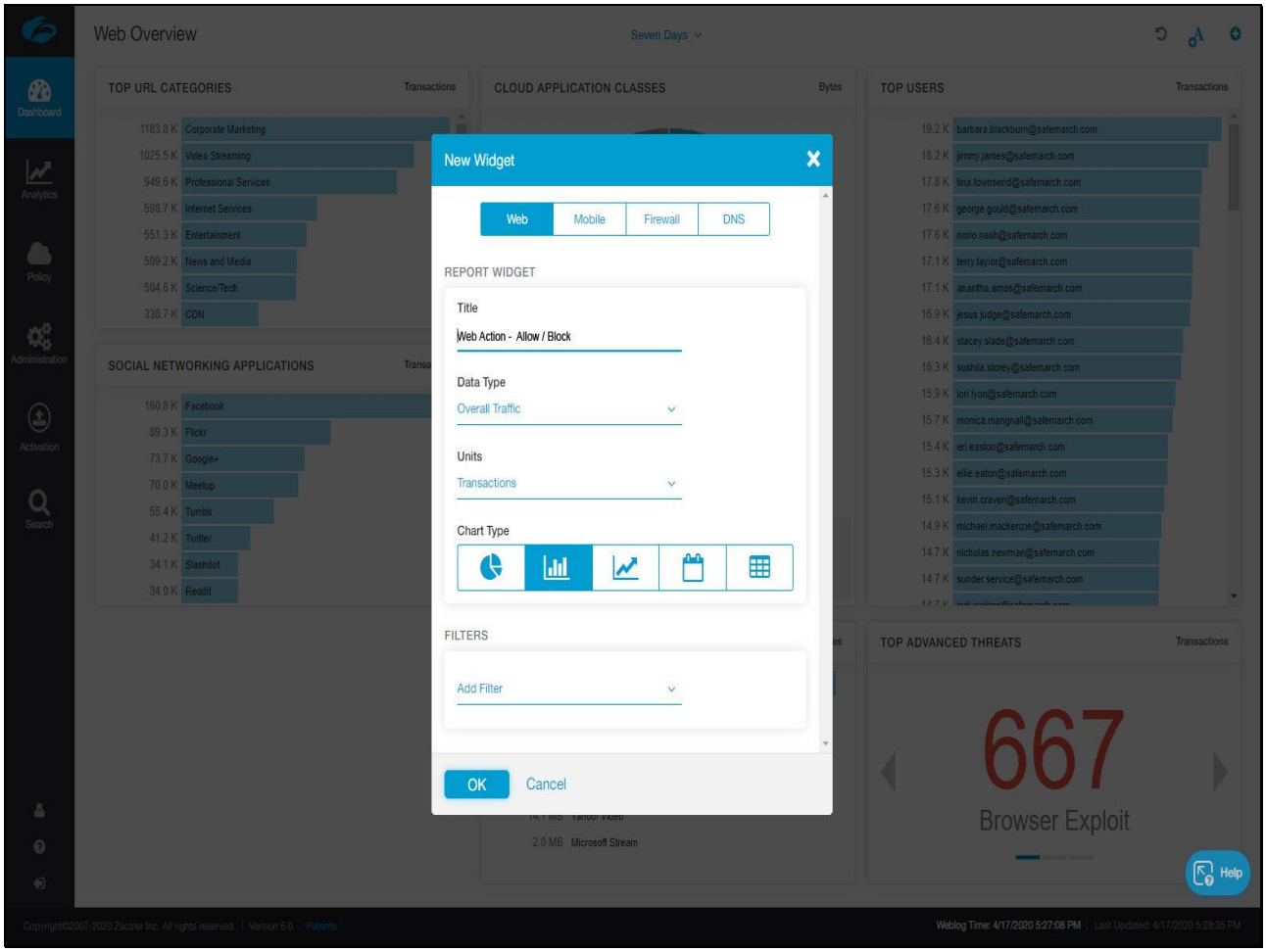
Slide 19 - Slide 19



Slide notes

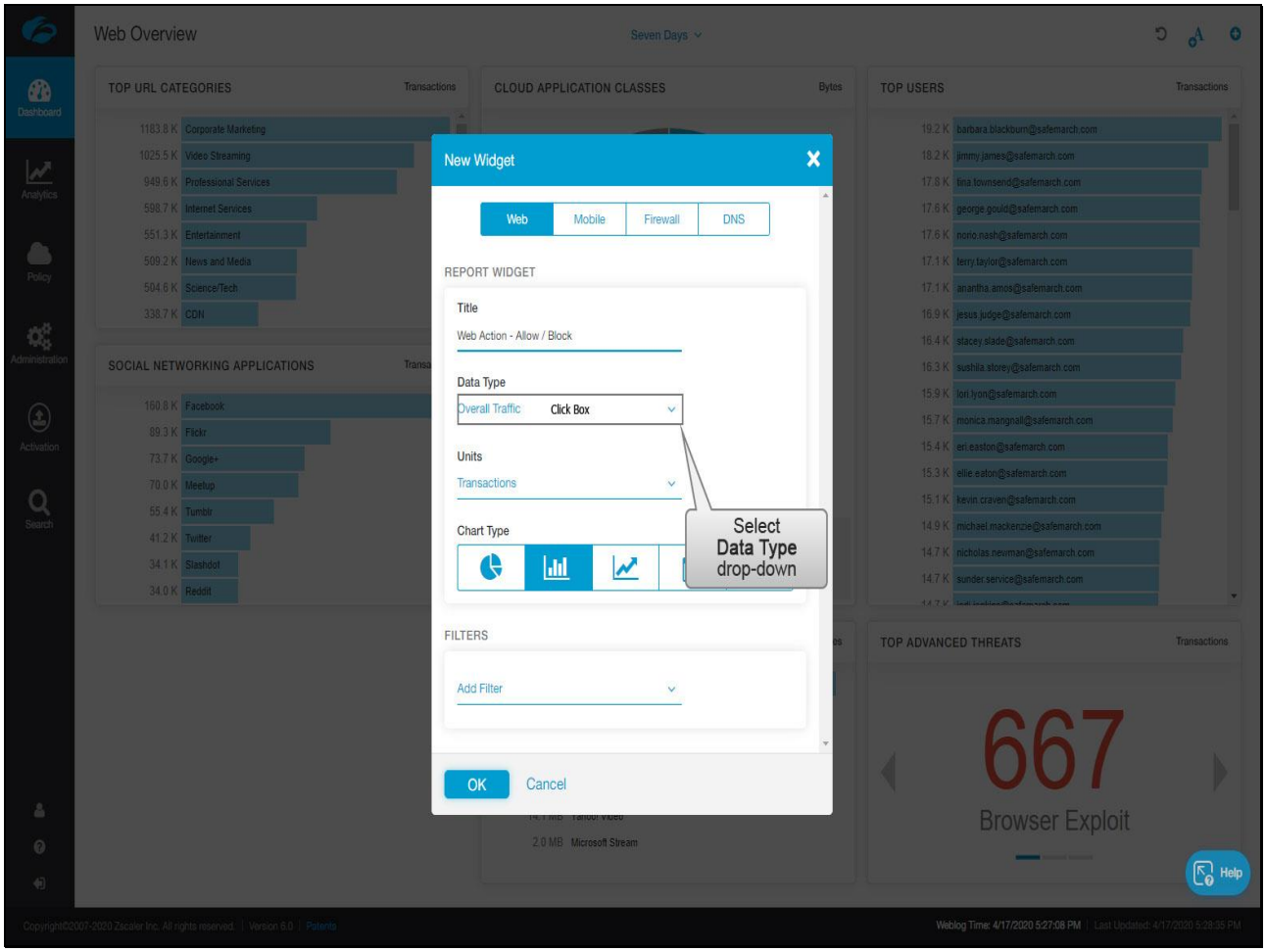
Provide a name for the new widget.

Slide 20 - Slide 20



Slide notes

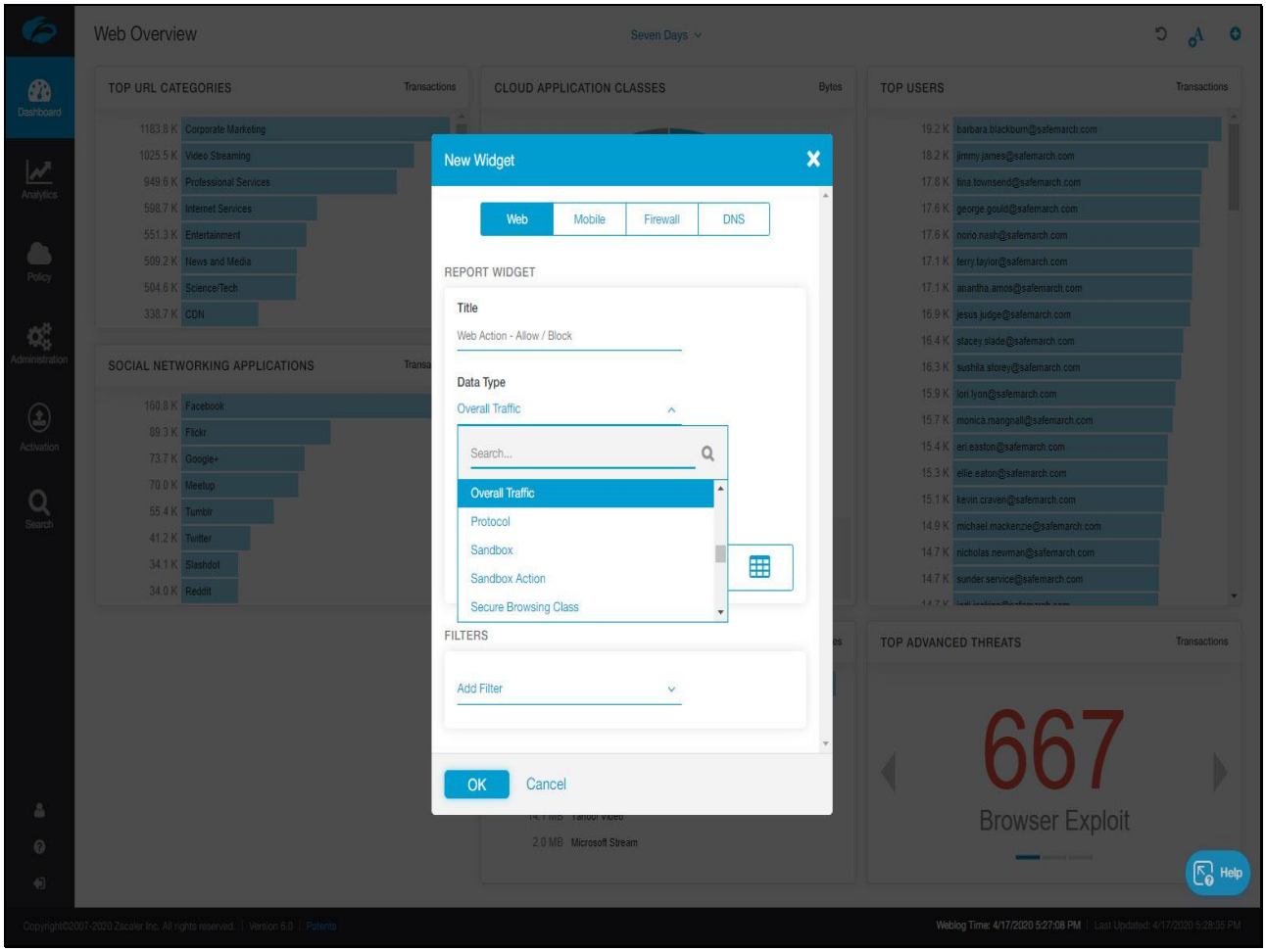
Slide 21 - Slide 21



Slide notes

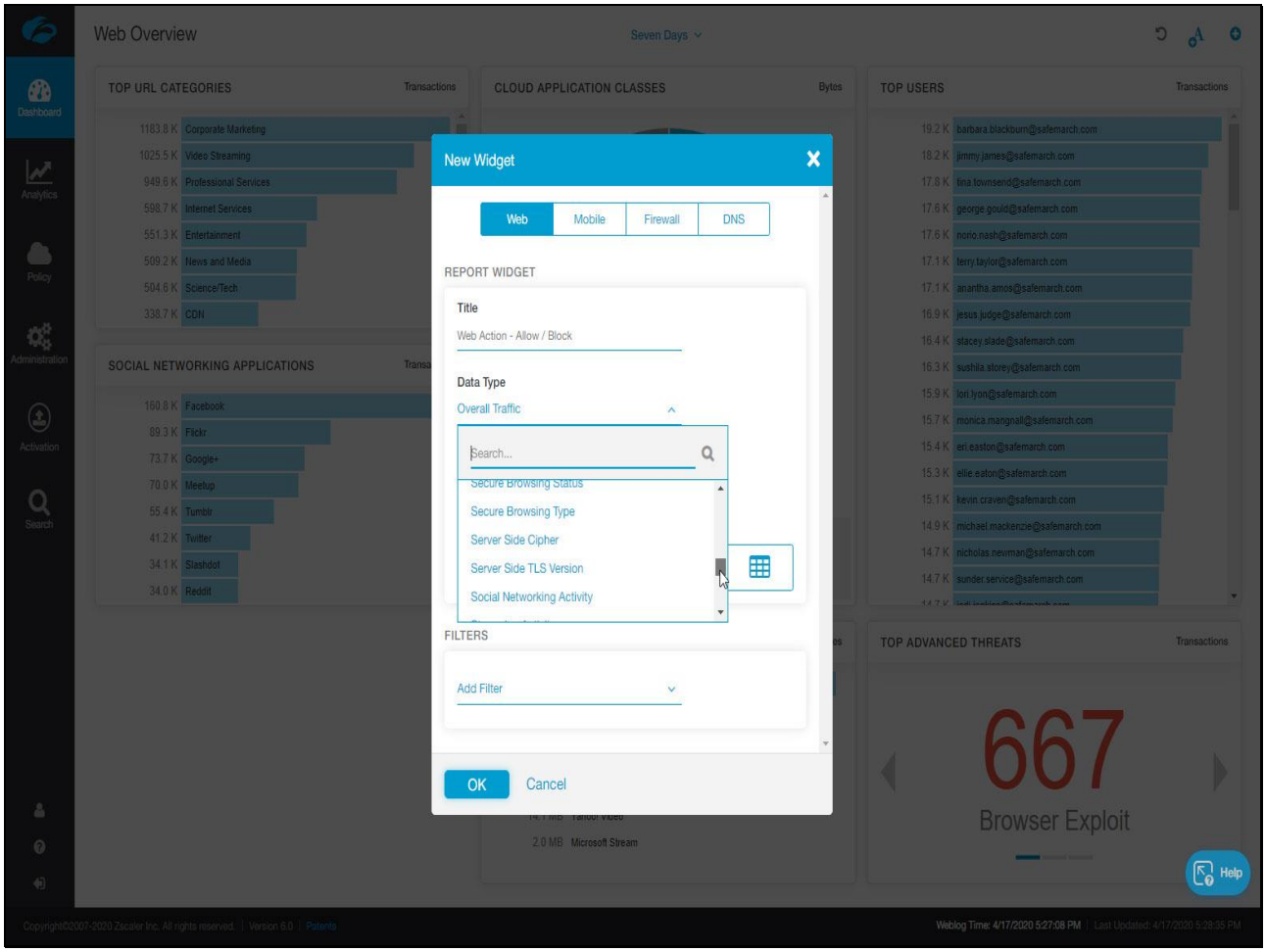
Select the **Data Type** drop-down window.

Slide 22 - Slide 22



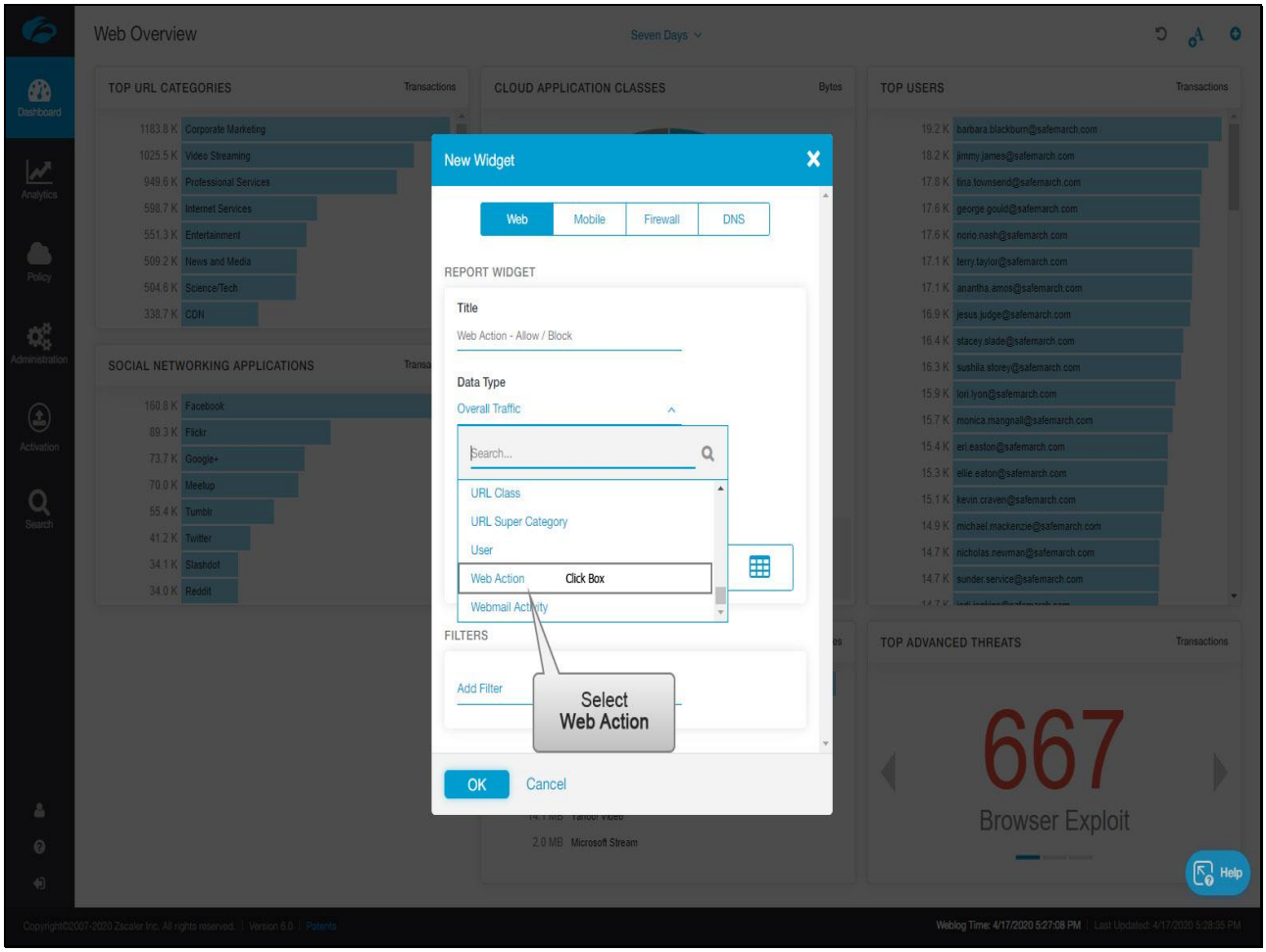
Slide notes

Slide 23 - Slide 23



Slide notes

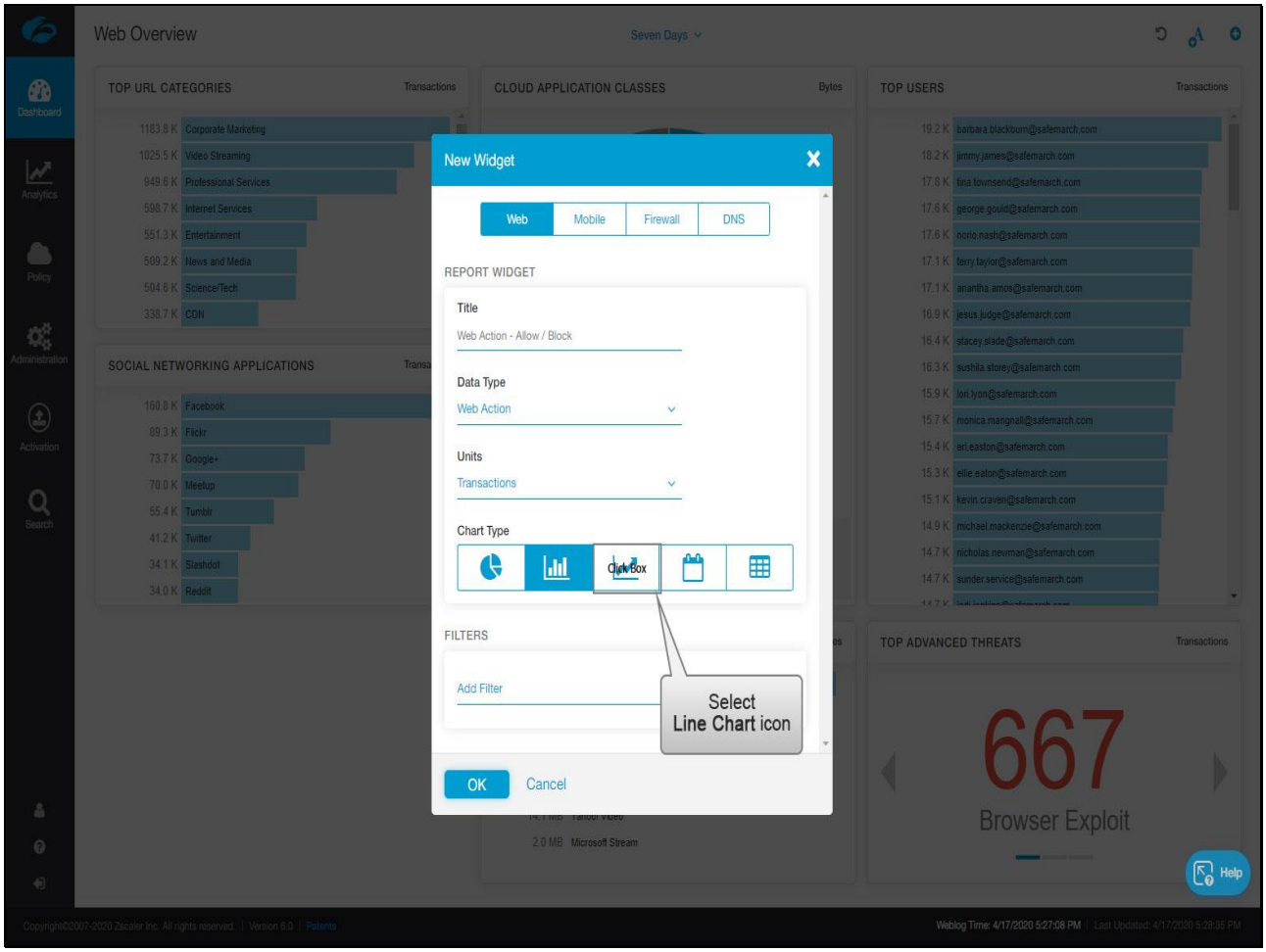
Slide 24 - Slide 24



Slide notes

Select “**Web Action**”.

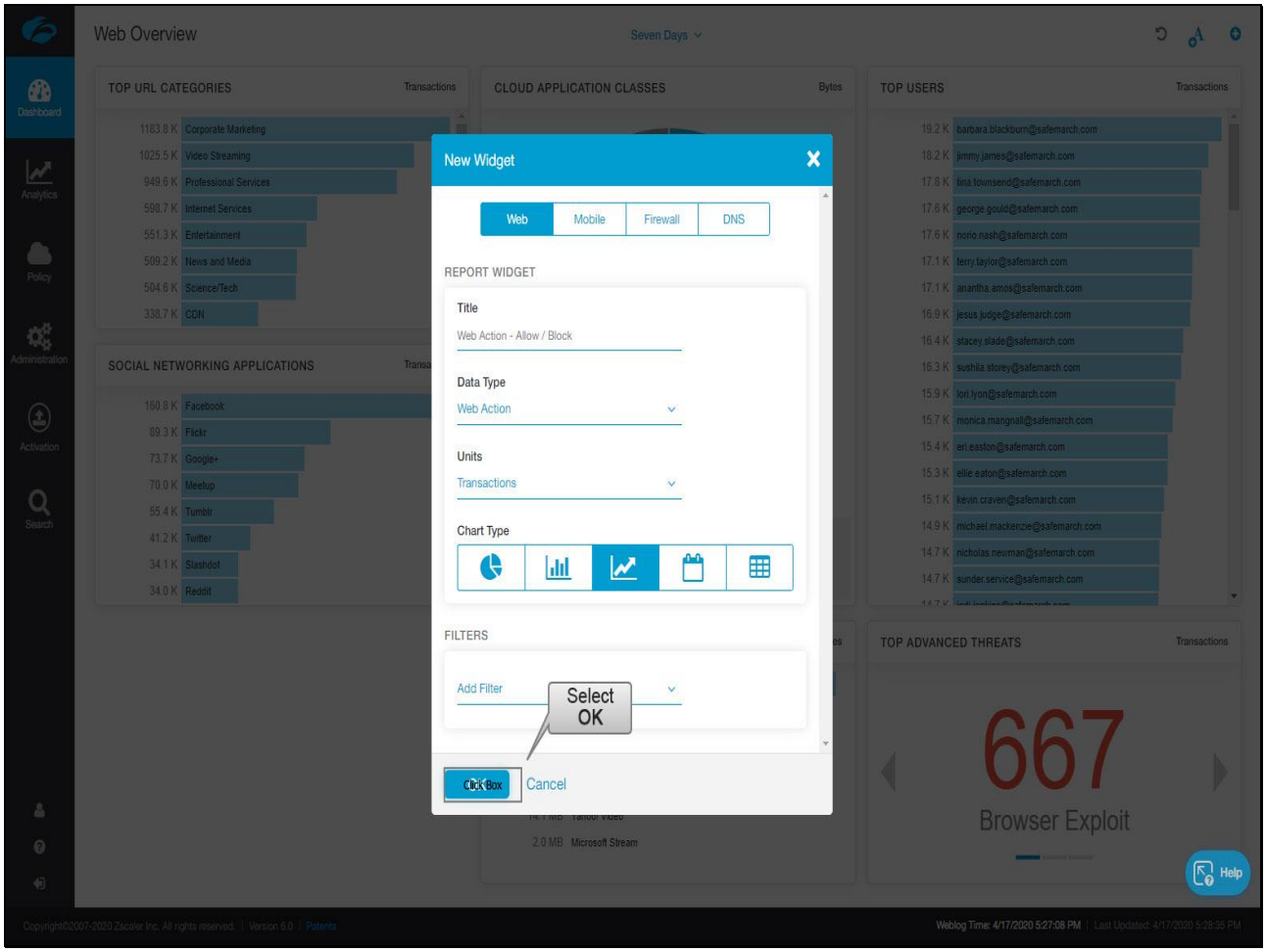
Slide 25 - Slide 25



Slide notes

Under Chart Type, select the **Line Chart** option.

Slide 26 - Slide 26



Slide notes

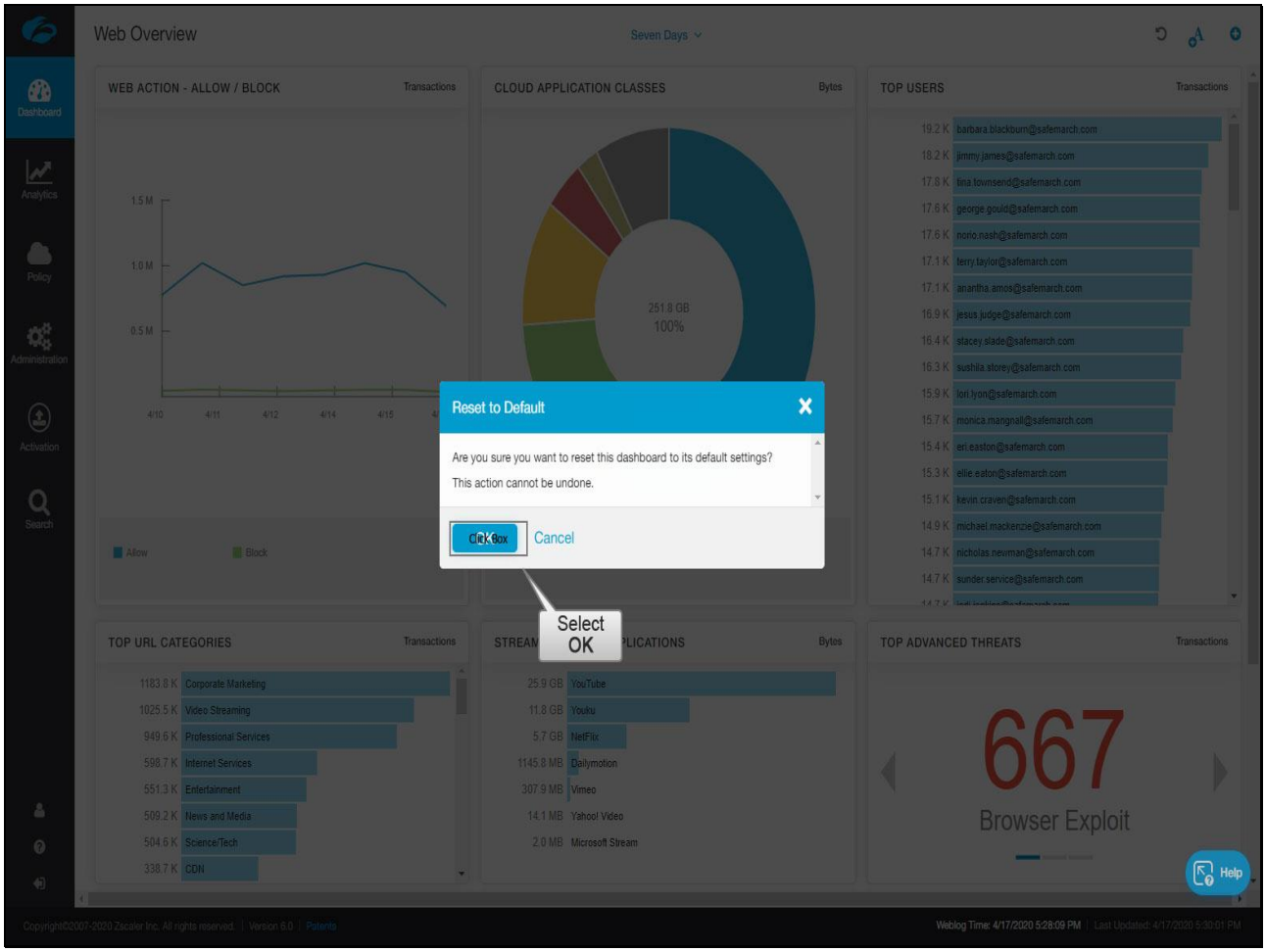
Then click "**OK**". No Activation is required when making changes to the dashboard or editing Widgets.

Slide 27 - Slide 27

Slide notes

If after making modifications to the dashboard you find that you are not happy with your results and don't remember exactly what you had changed along the way you can always reset the Dashboard to its' default state. To reset the Dashboard to the default setting click the "**Reset icon**" near the upper right corner of the dashboard.

Slide 28 - Slide 28



Slide notes

Then read the warning message and click **OK.**

Slide 29 - Slide 29

Slide notes

Slide 30 - System defined reports

Slide notes

As a new Zscaler administrator it is important for you to quickly asses where your current security posture stands and what threats exist on your network. Once you understand what threats exist you can begin to address them. Using the system defined reports is an excellent way to begin.

Slide 31 -

Executive Report

Slide notes

Slide 32 - Slide 32

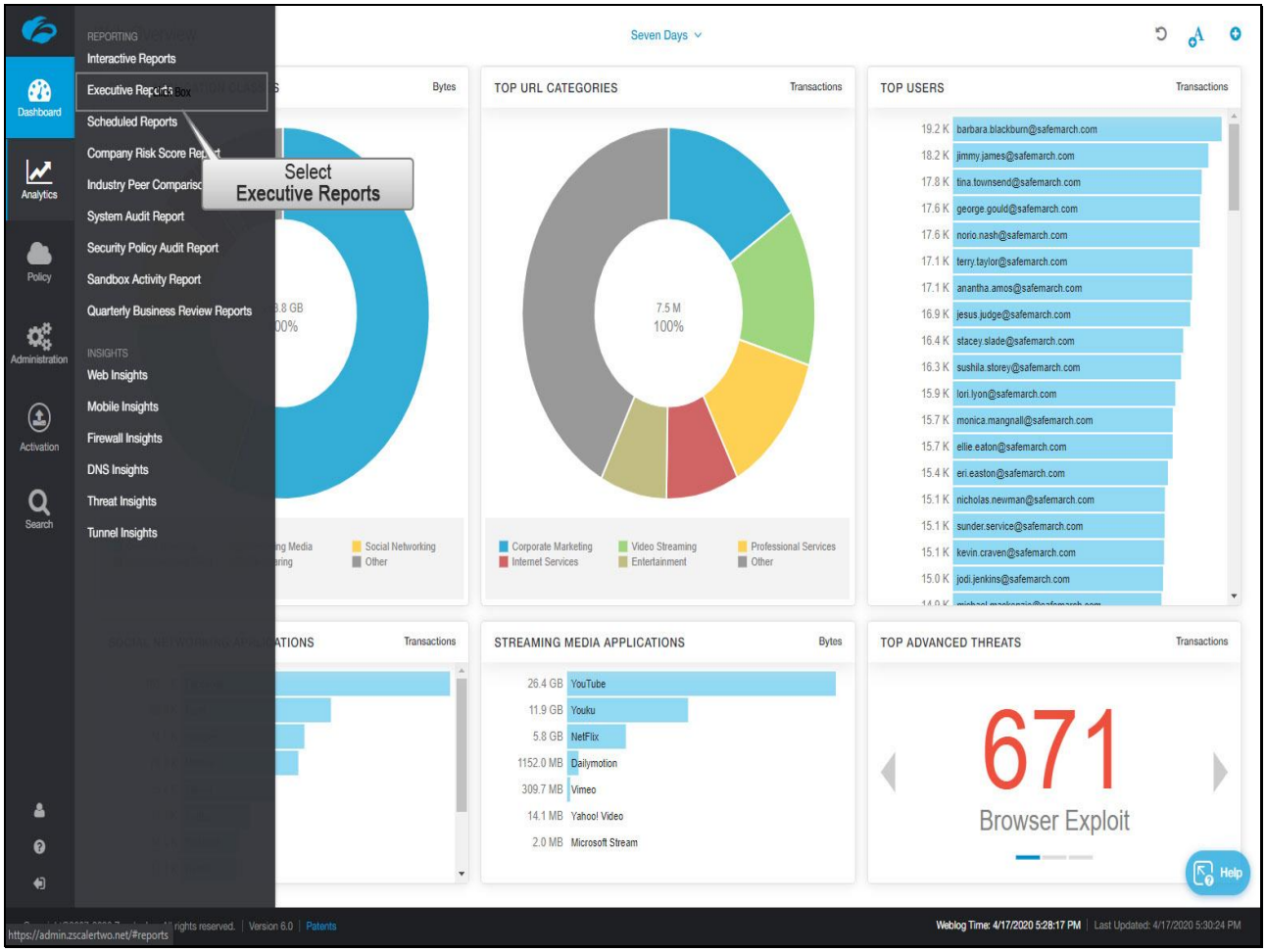
Slide notes

The first report you want to review, once Zscaler has been inline and examining your organizations traffic for some time, is the Executive Report. It provides a quick snapshot of your company's security posture and highlights the value that you derive from the Zscaler platform.

It displays information like the number of security threats or policy violations that the Zscaler service detected for your organization. The Executive Report contains information that is tailored for your executive staff; however, it is also invaluable for the new Zscaler admin.

Begin by clicking on the **Analytics tab**.

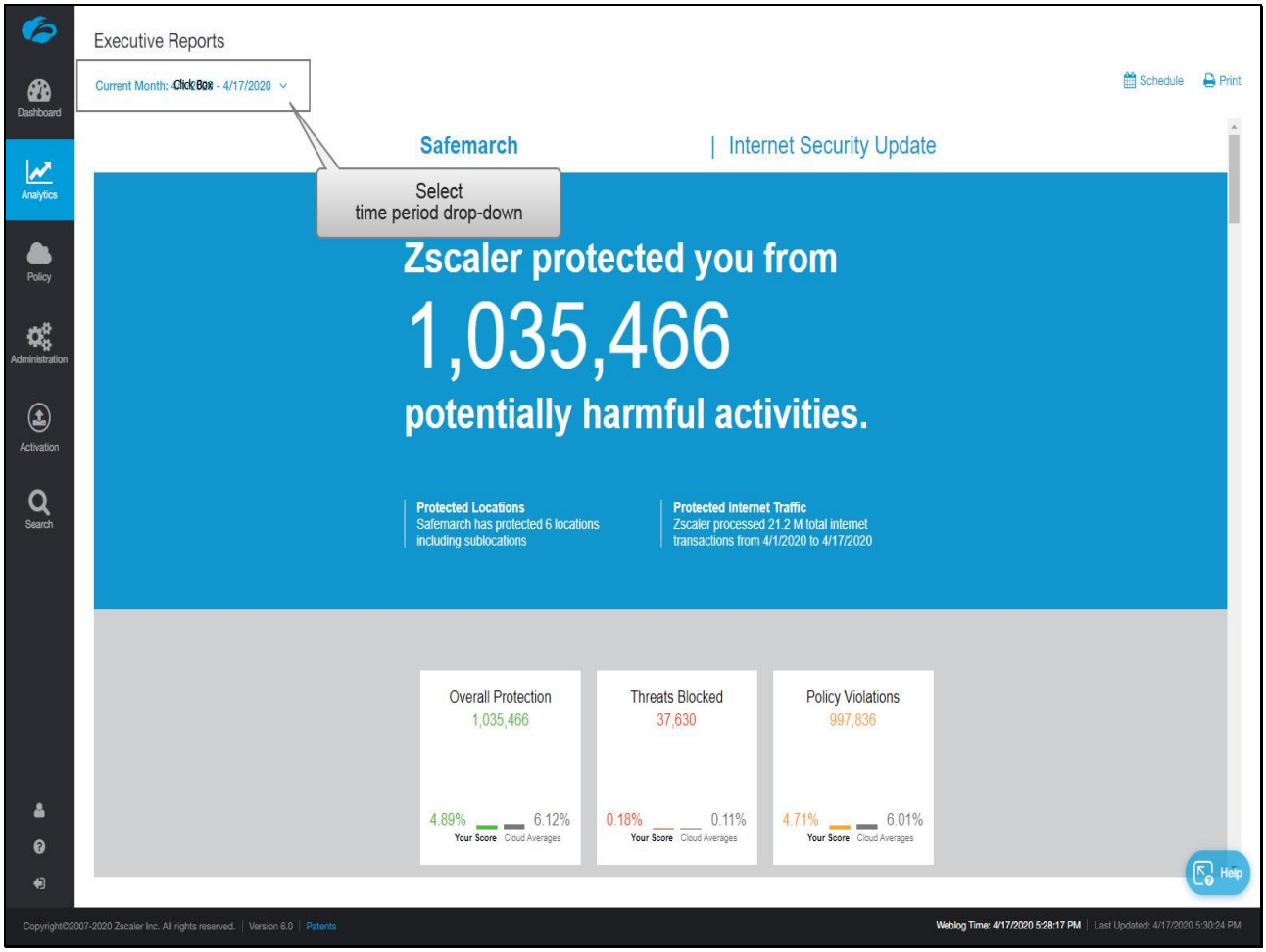
Slide 33 - Slide 33



Slide notes

Then click on **Executive Report**.

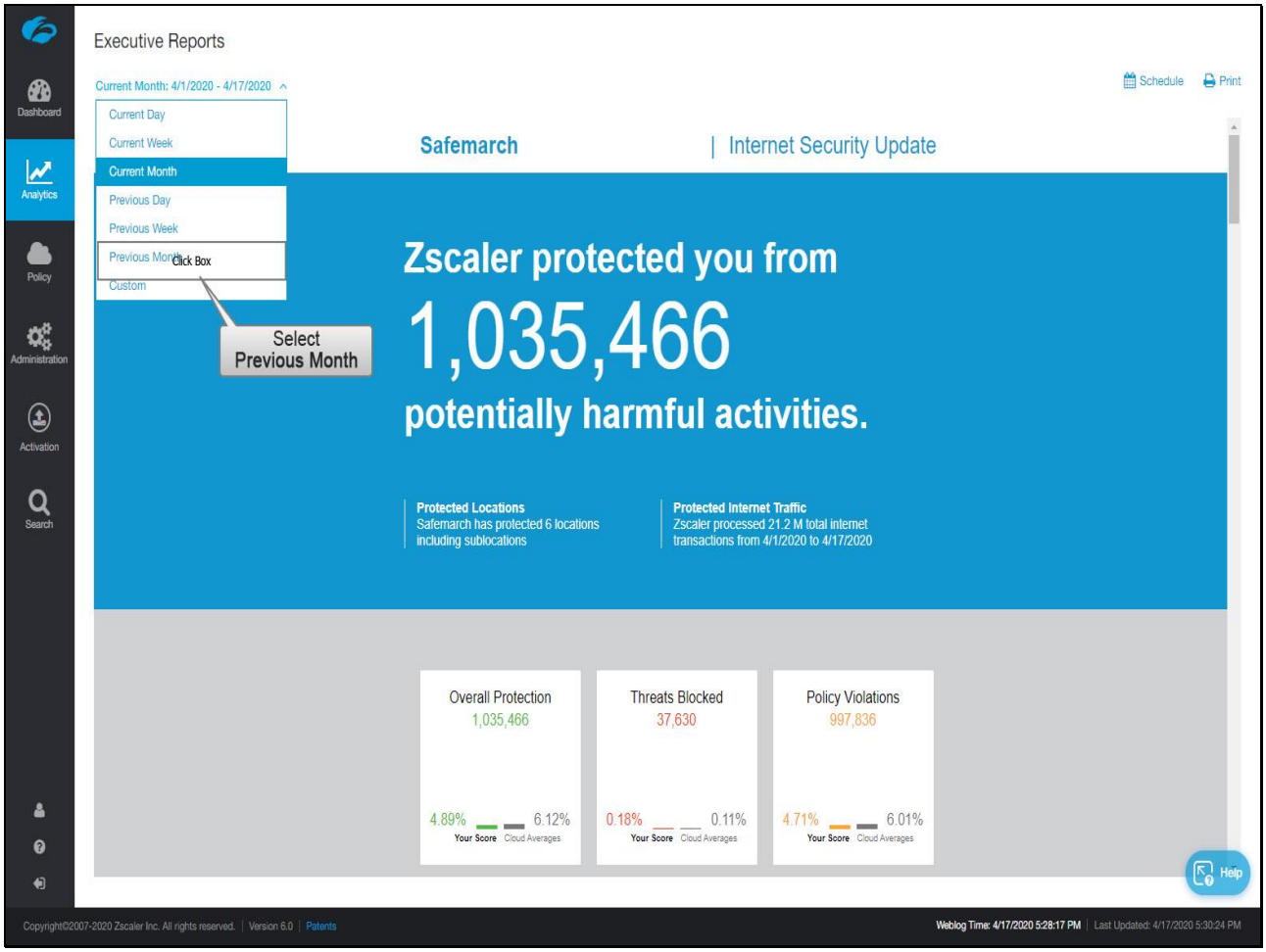
Slide 34 - Slide 34



Slide notes

Choose the date range that you want the data to be compiled for.

Slide 35 - Slide 35

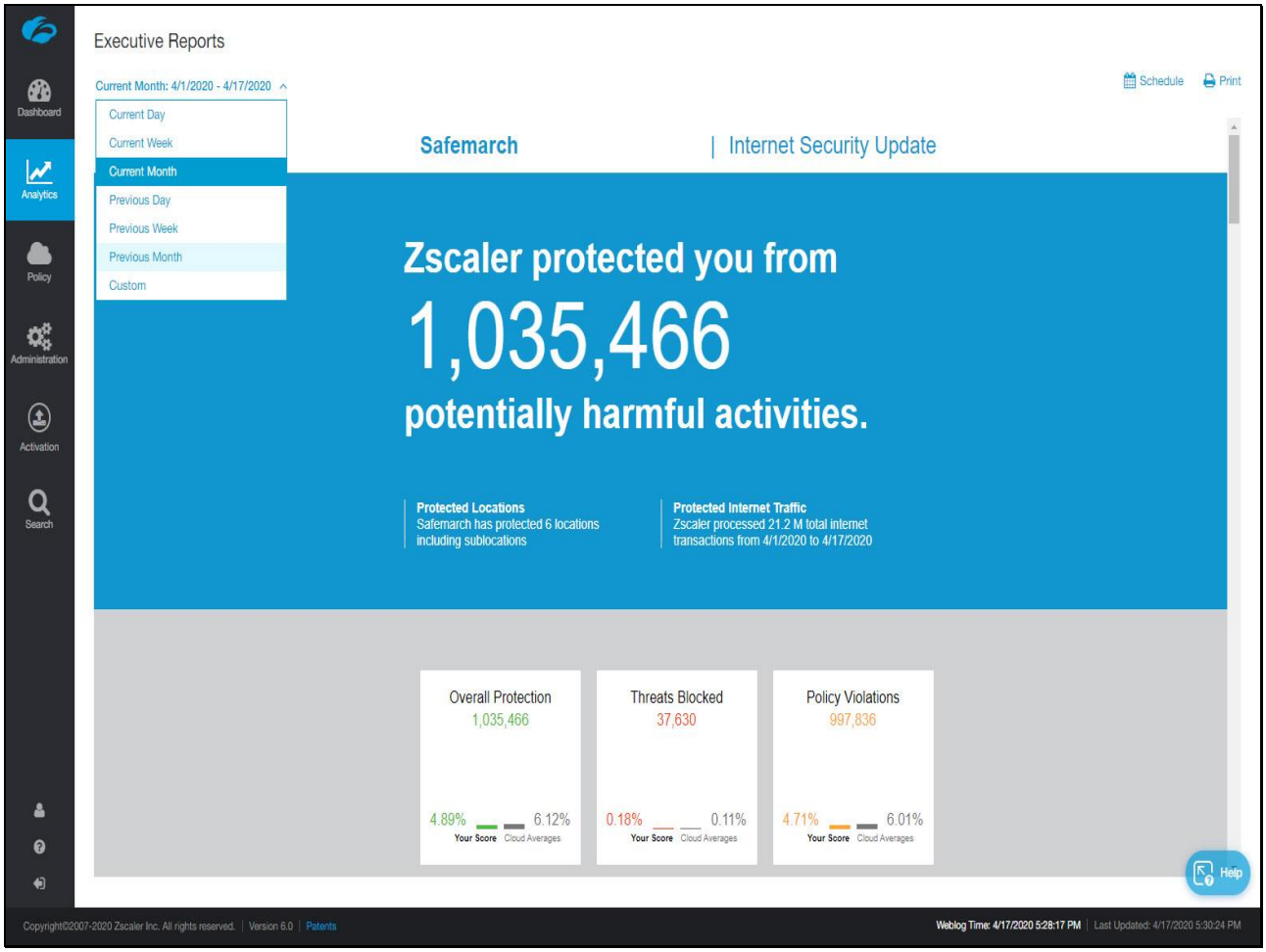


Slide notes

Choose the date range that you want the data to be compiled for.

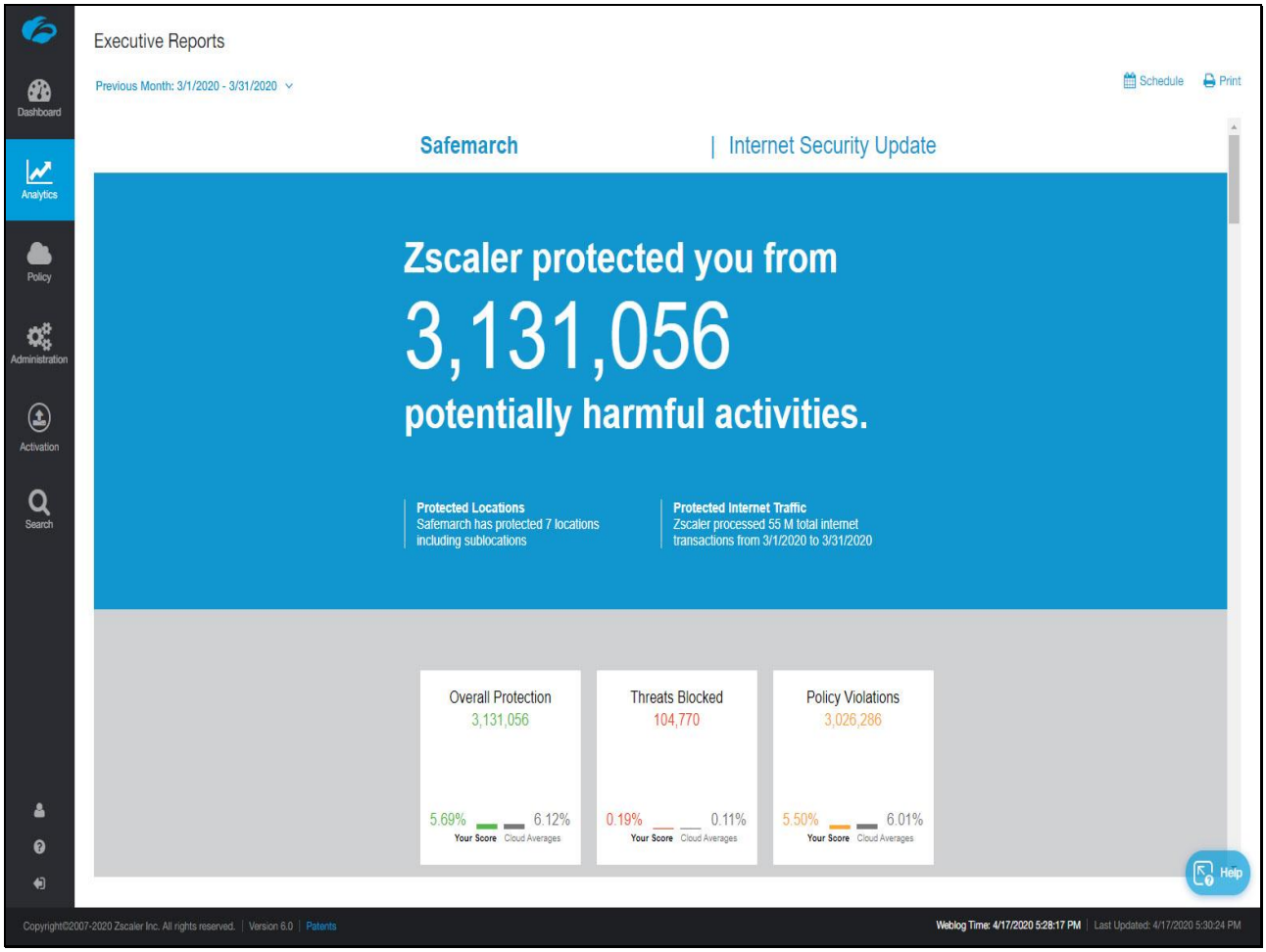
Select **Previous Month**.

Slide 36 - Slide 36



Slide notes

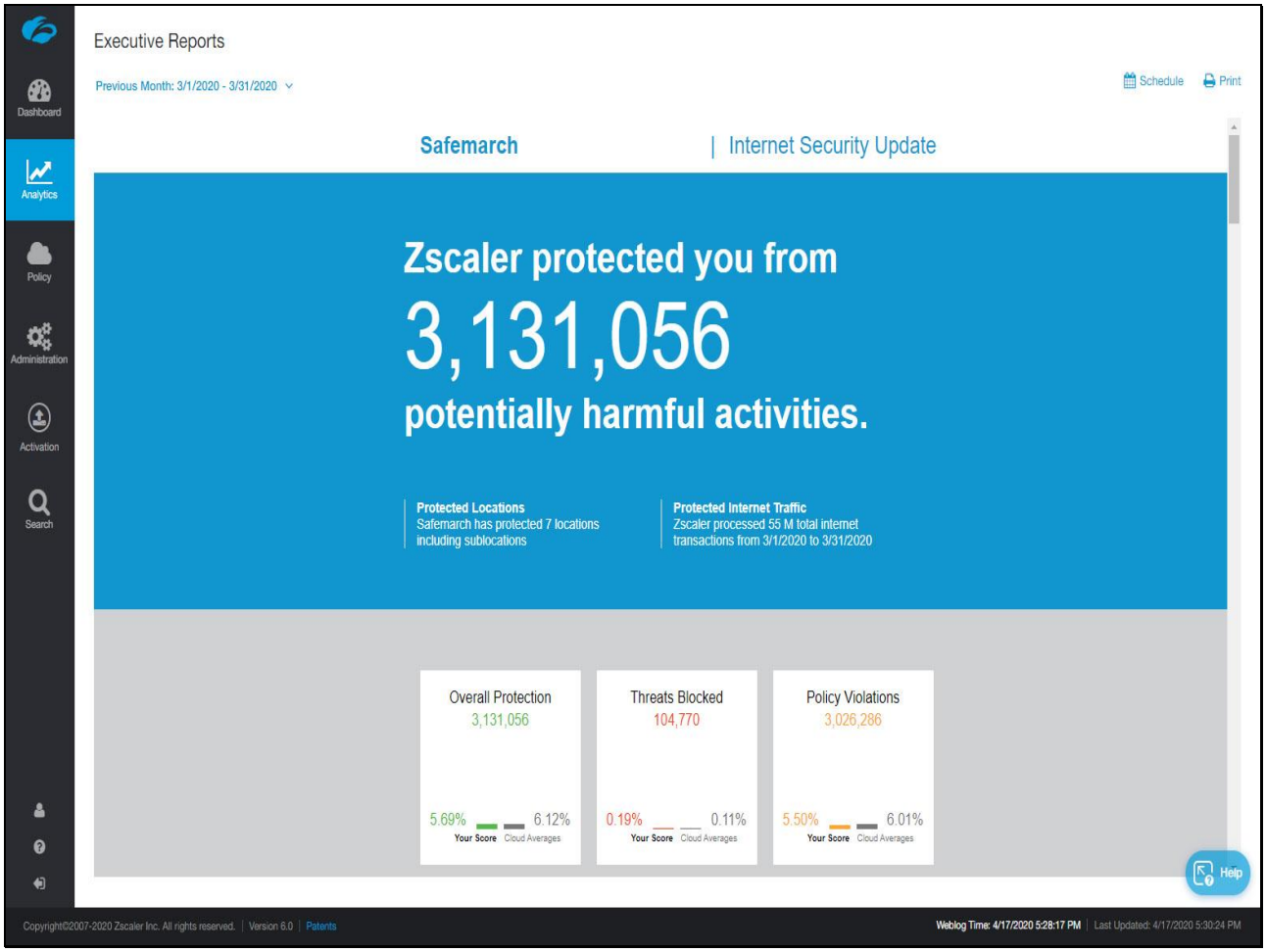
Slide 37 - Slide 37



Slide notes

You can simply view the report on your screen or print a copy.

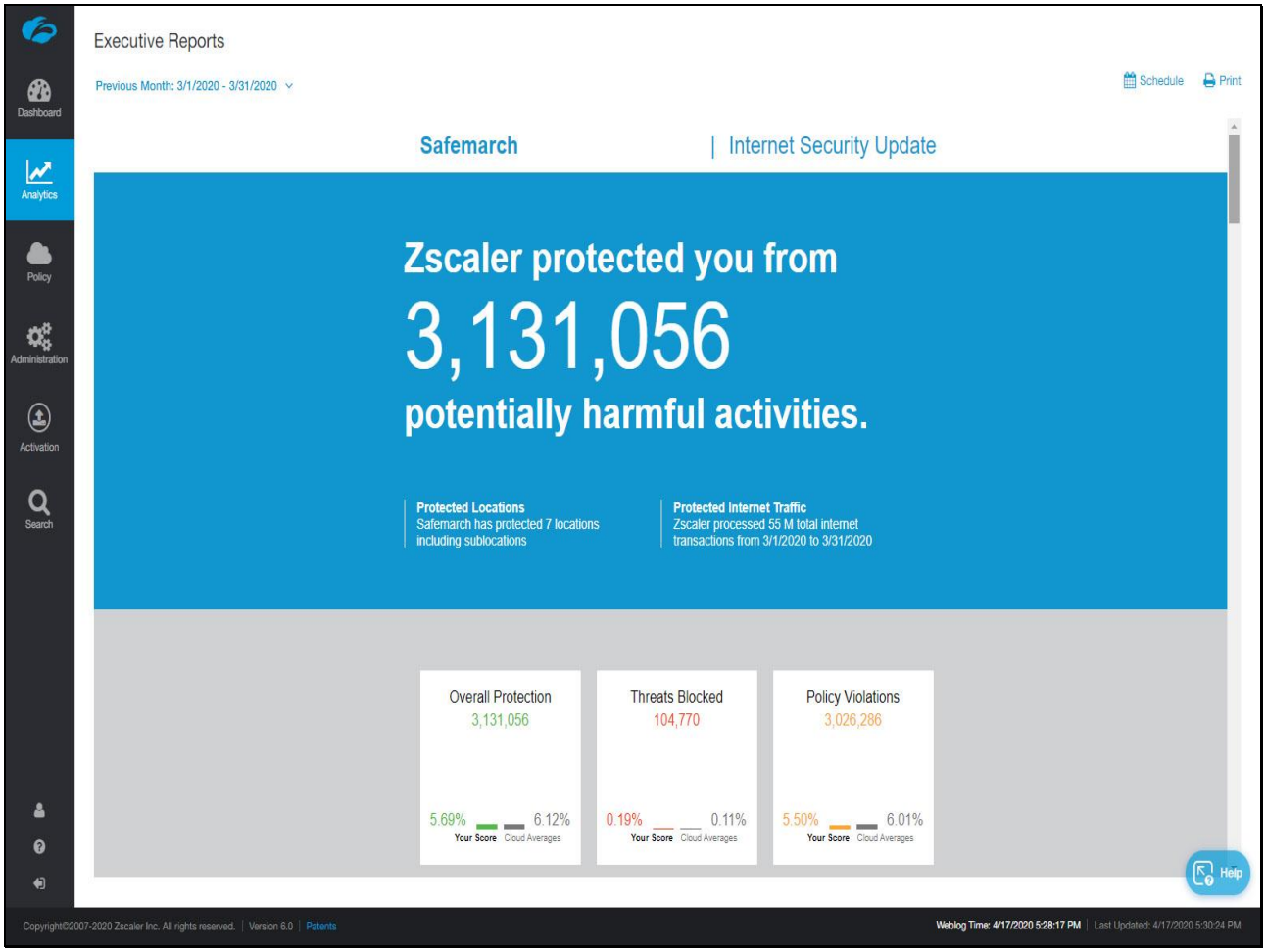
Slide 38 - Slide 38



Slide notes

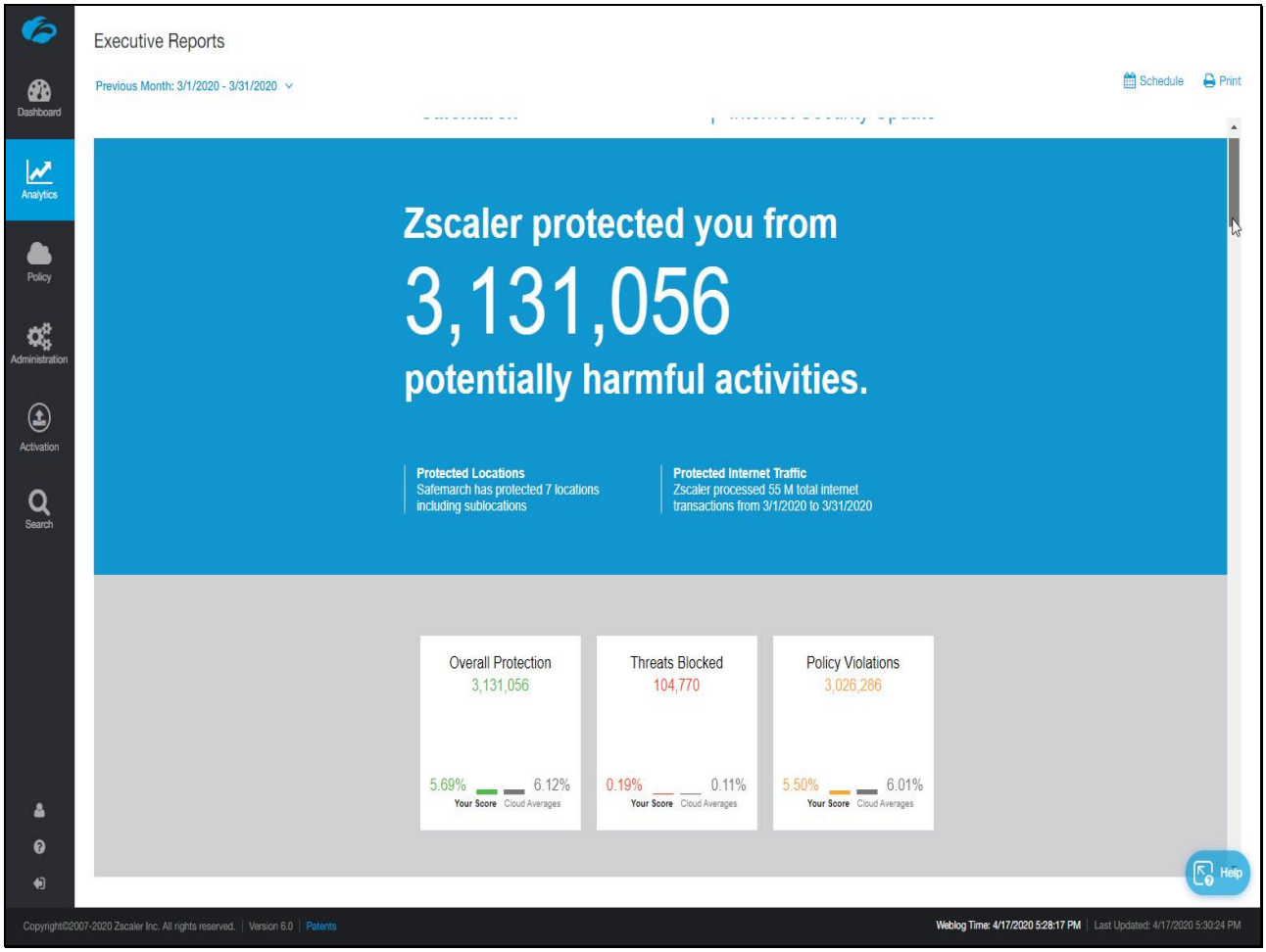
This first section describes how many transactions and threats were blocked and how many policy violations took place during the time frame you selected for the report.

Slide 39 - Slide 39



Slide notes

Slide 40 - Slide 40



Slide notes

Slide 41 - Slide 41

Slide notes

Next, we examine Advanced threats. One item we focus on is the Botnet callout and spyware callback. If the report shows that a lot of callbacks are being blocked by Zscaler that is both a good thing and a bad thing. It is good that, while the device is infected, Zscaler is able to identify and block the call.

Awareness of this activity is the key to this report. Now that the Administrator is aware of this activity remediation can take place. Infected devices can be tracked using the reporting and analytics capabilities built into the Zscaler platform.

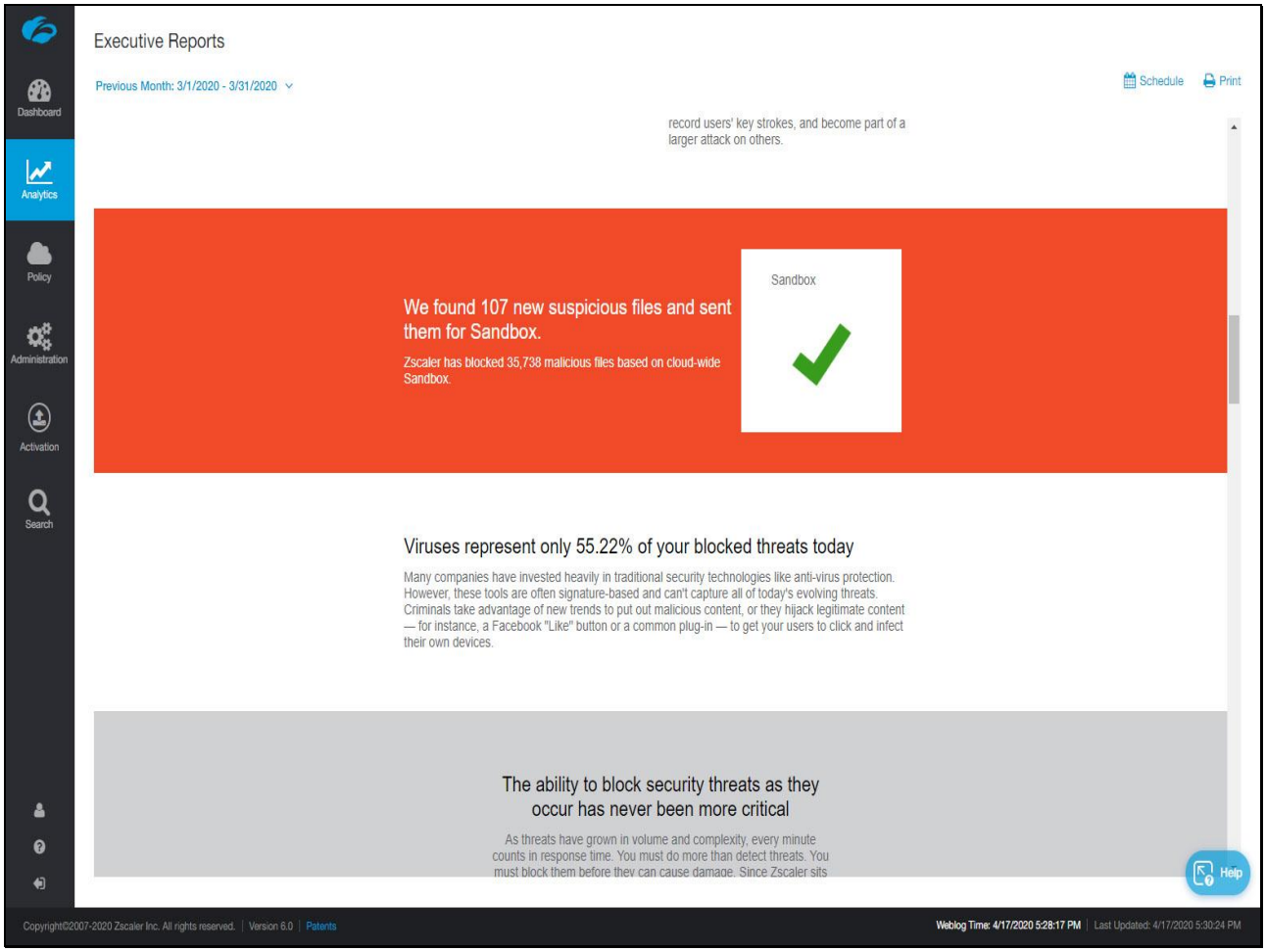
Slide 42 - Slide 42

Slide notes

Slide 43 - Slide 43

Slide notes

Slide 44 - Slide 44



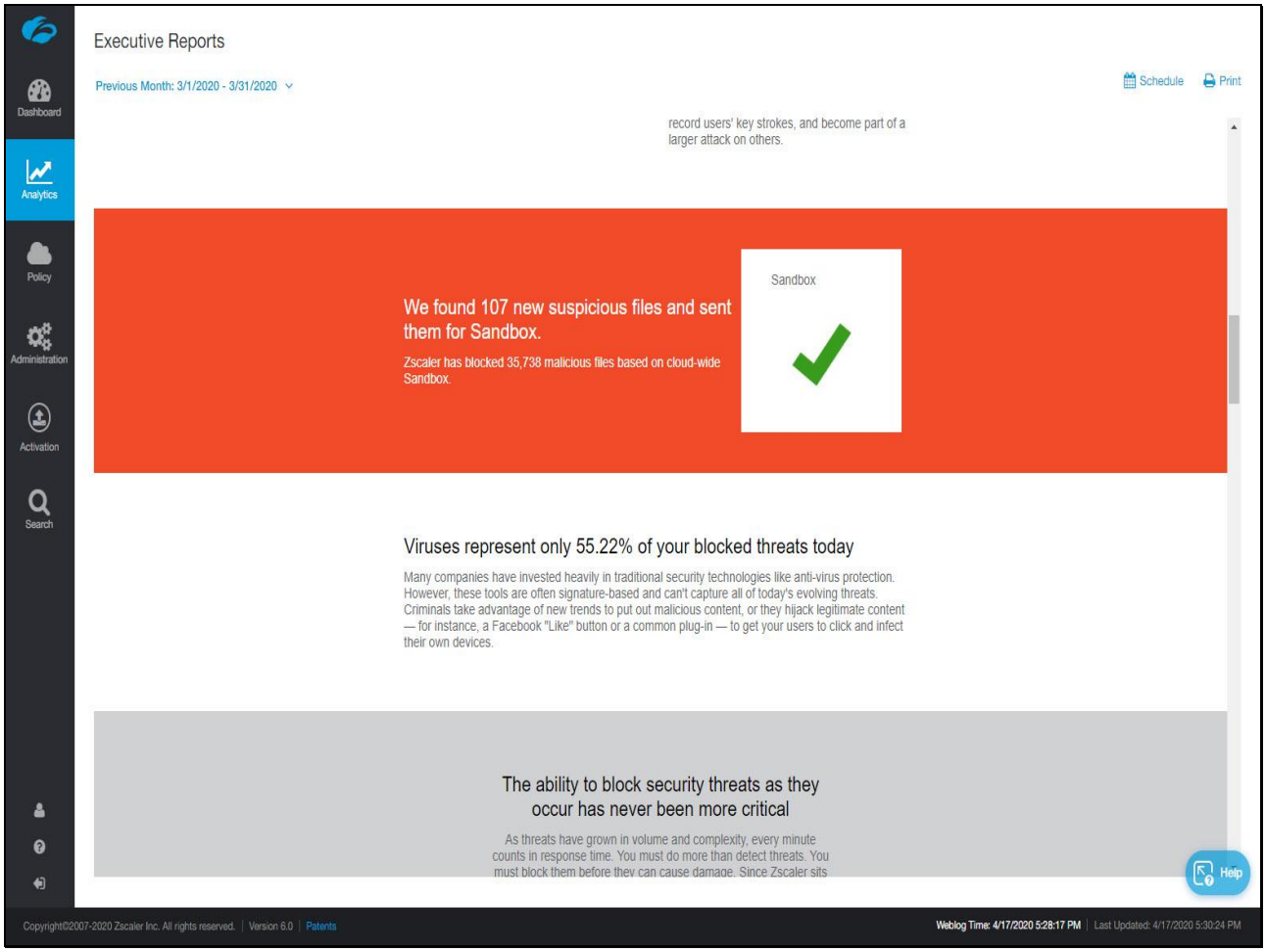
Slide notes

Sandboxing suspicious files and detonating them for inspection before allowing the file to be downloaded by your employees is key to preventing infection. This part of the report demonstrates how effective Sandboxing is in an organization. In this case, 107 files that have never been seen by Zscaler before were sent to the Sandbox for detonation and examination.

These files, if allowed to be downloaded, could have cause infection. Also notice, that within the time period for this report, almost 36,000 suspicious files were found cloud wide.

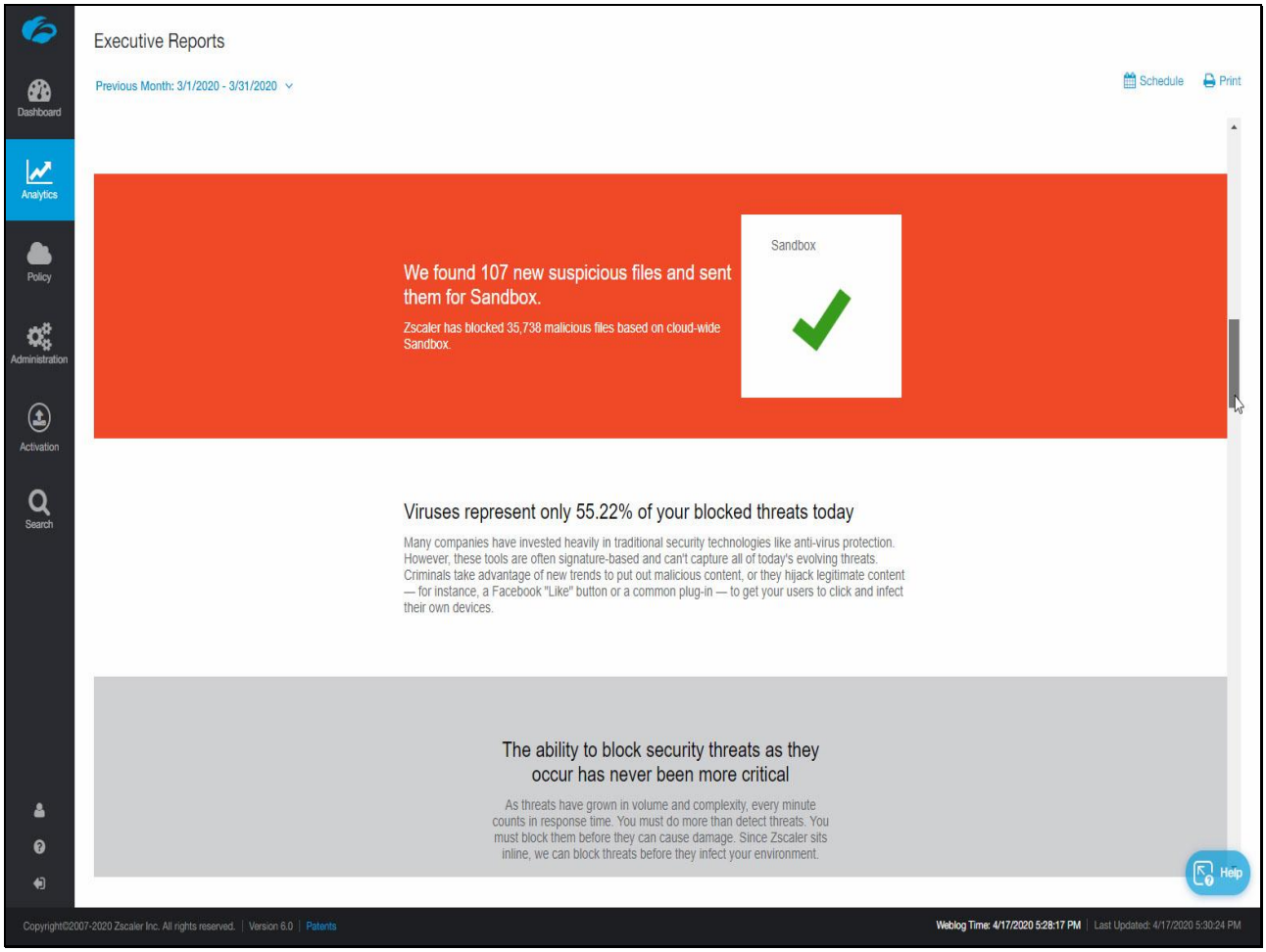
This is important as when a file is found to be malicious the MD5 is recorded and any time there is a matching MD5 on another file it is automatically flagged and quarantined – even if that file was seen by a different customer. All Zscaler customers benefit when one customer finds a malicious file.

Slide 45 - Slide 45



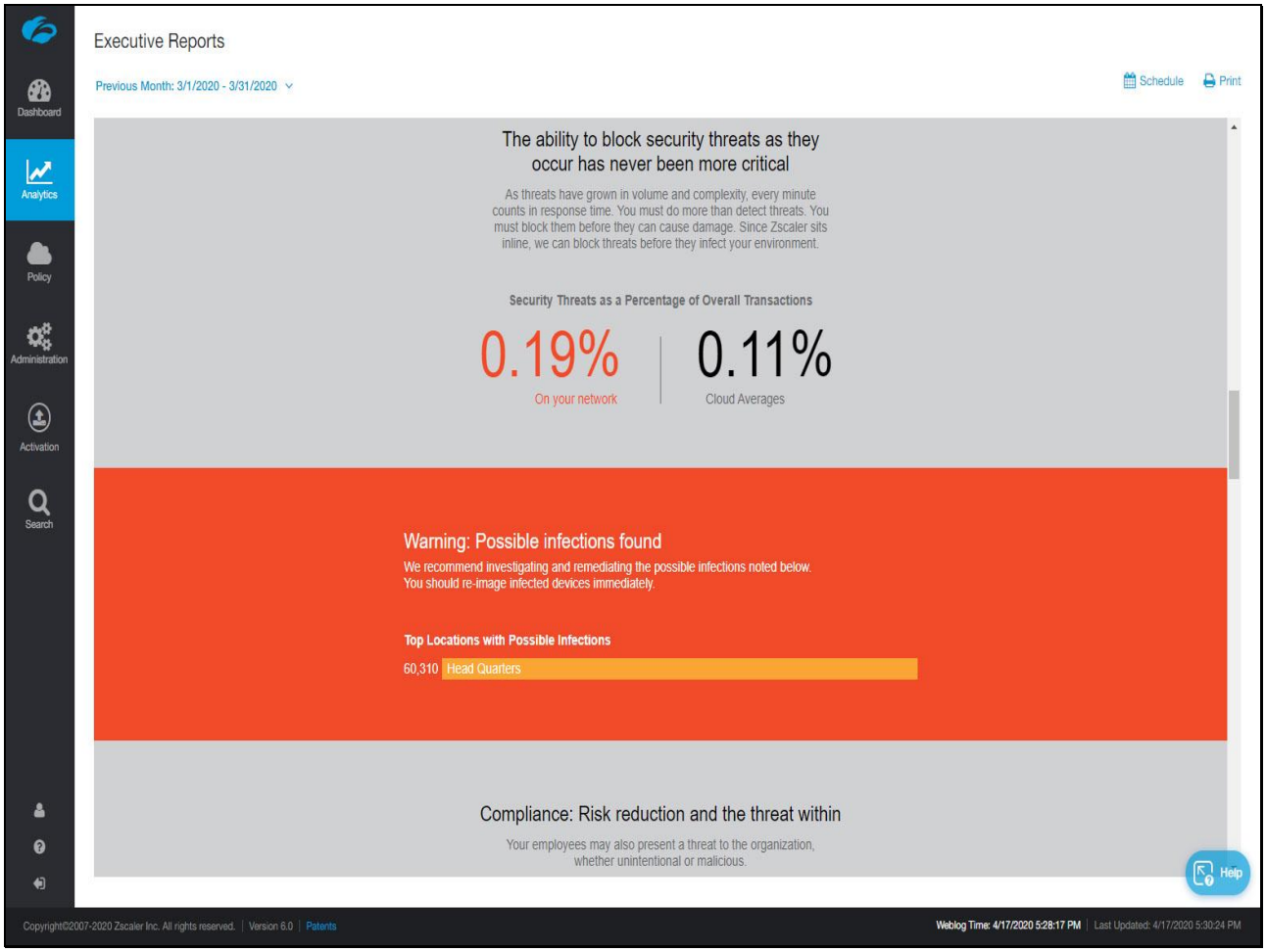
Slide notes

Slide 46 - Slide 46



Slide notes

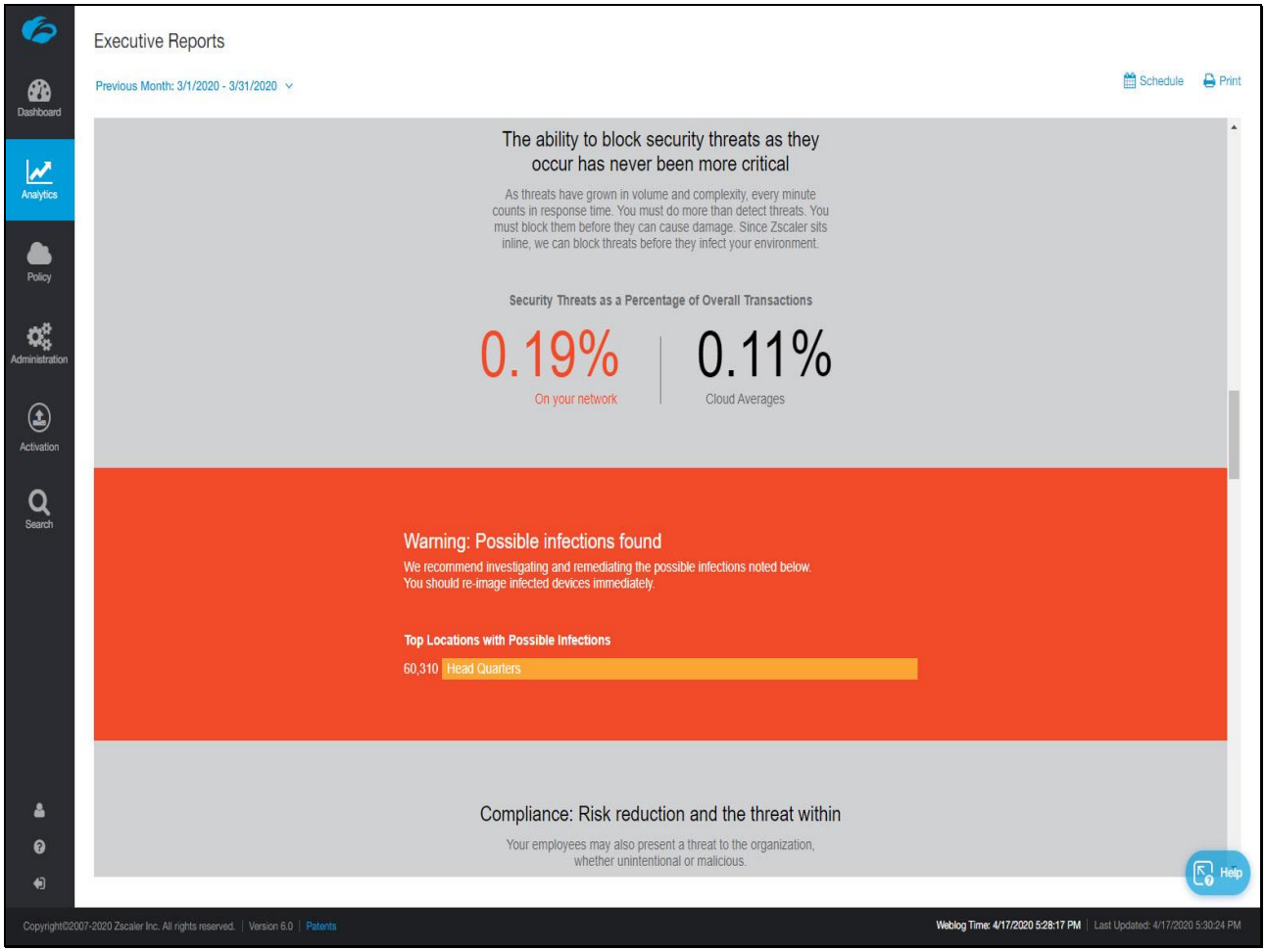
Slide 47 - Slide 47



Slide notes

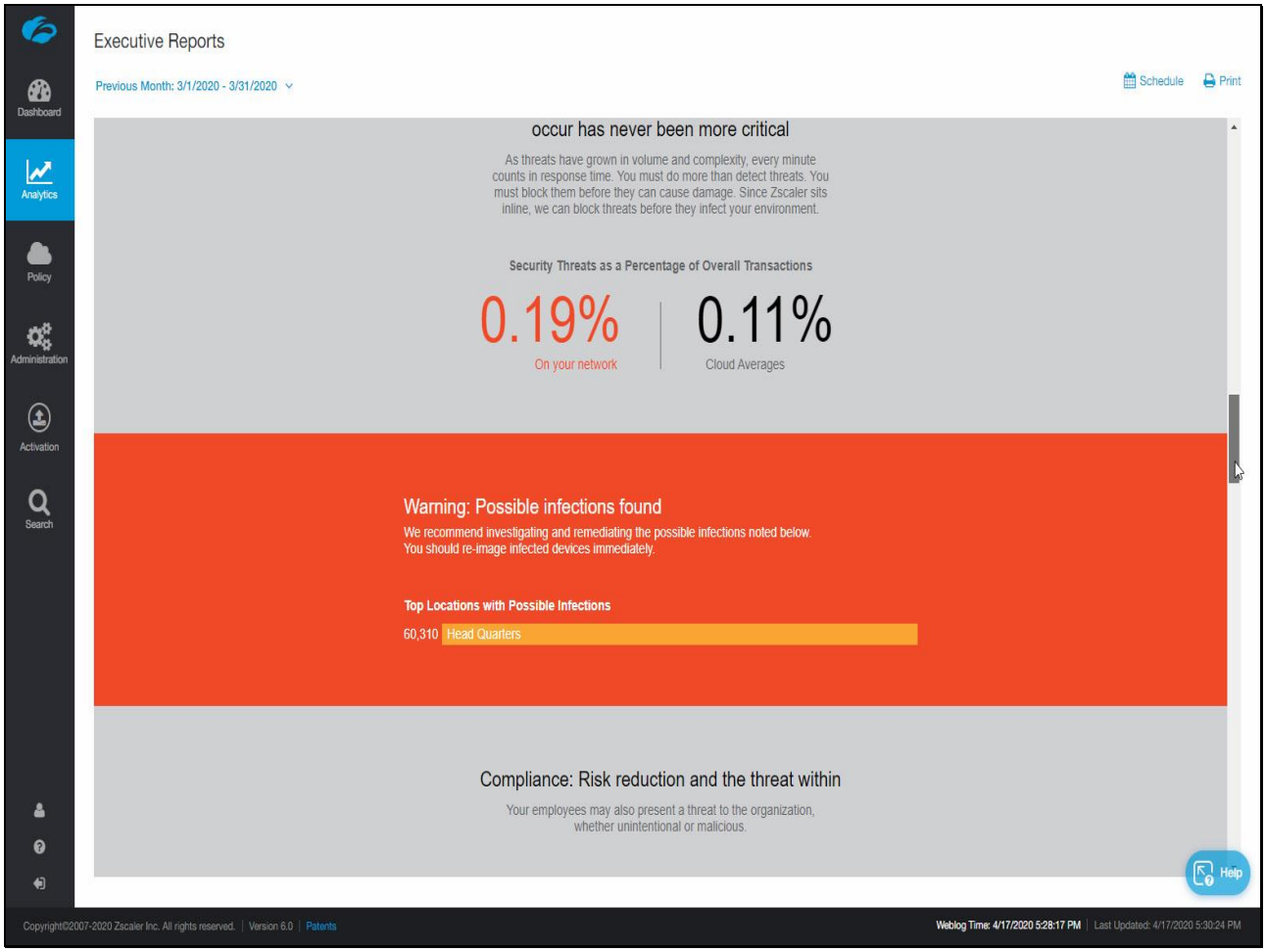
Next, we show the top infected users or locations. Knowing where the problem spots are enables the Administrator to be more effective.

Slide 48 - Slide 48



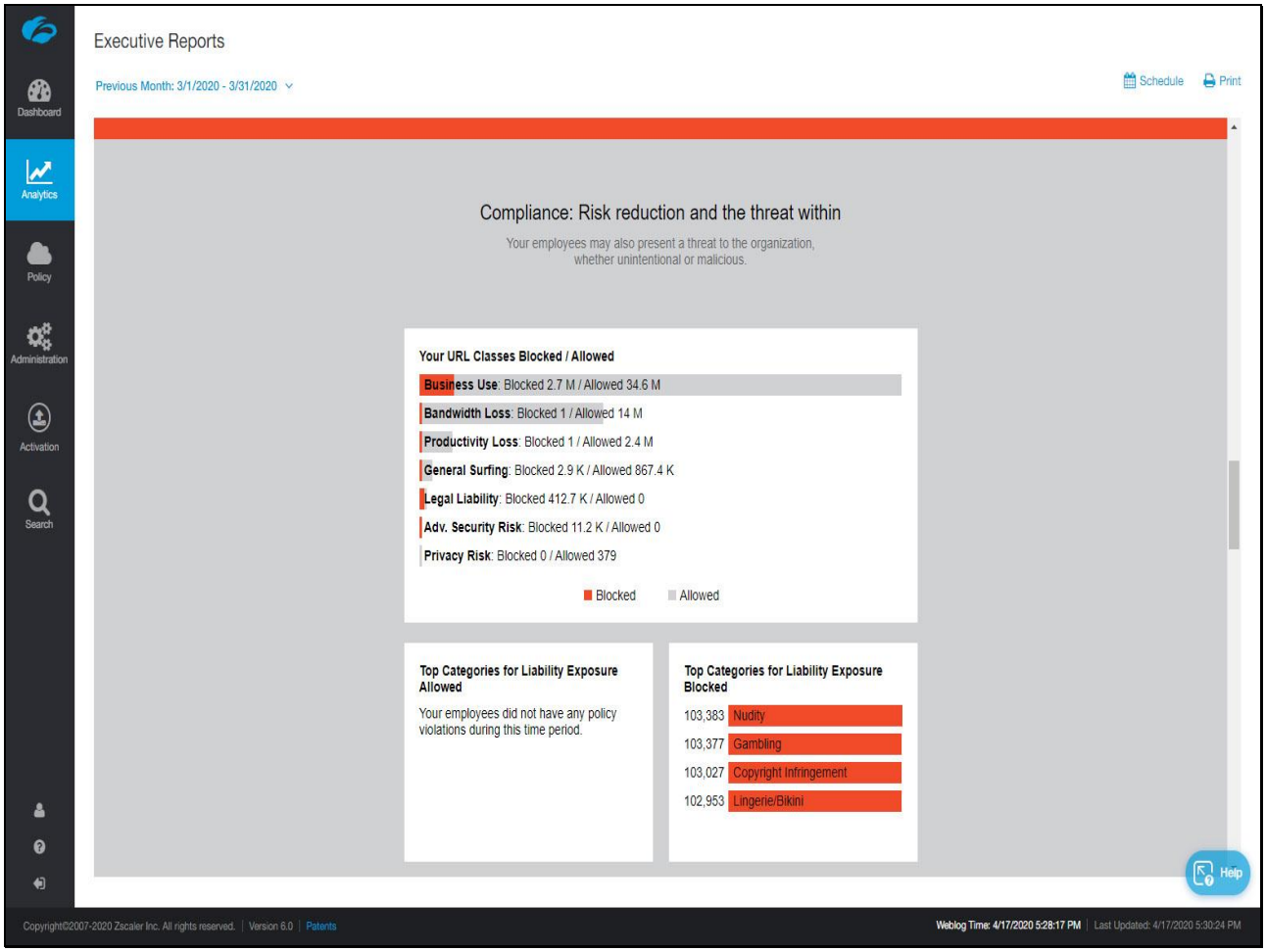
Slide notes

Slide 49 - Slide 49



Slide notes

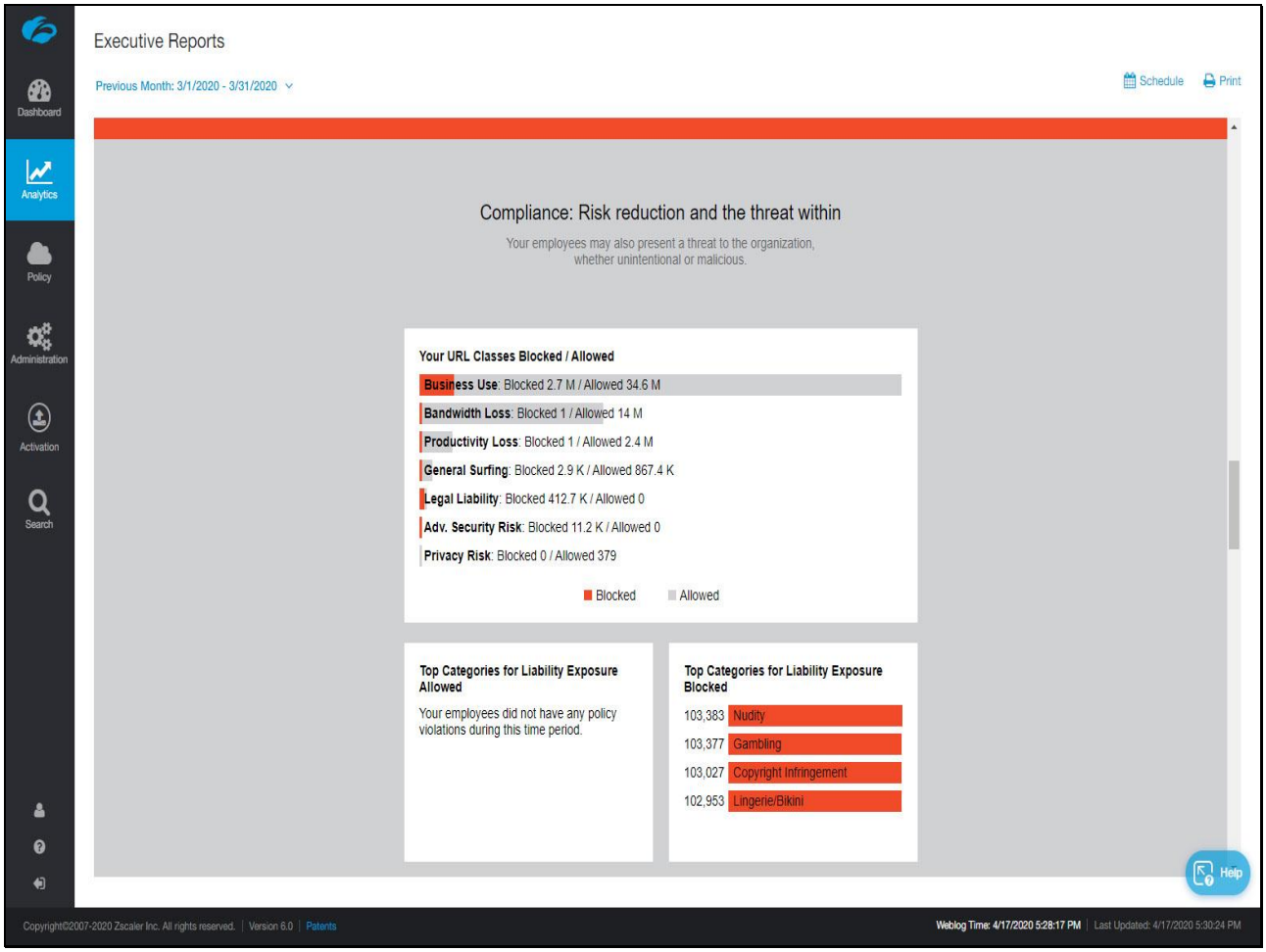
Slide 50 - Slide 50



Slide notes

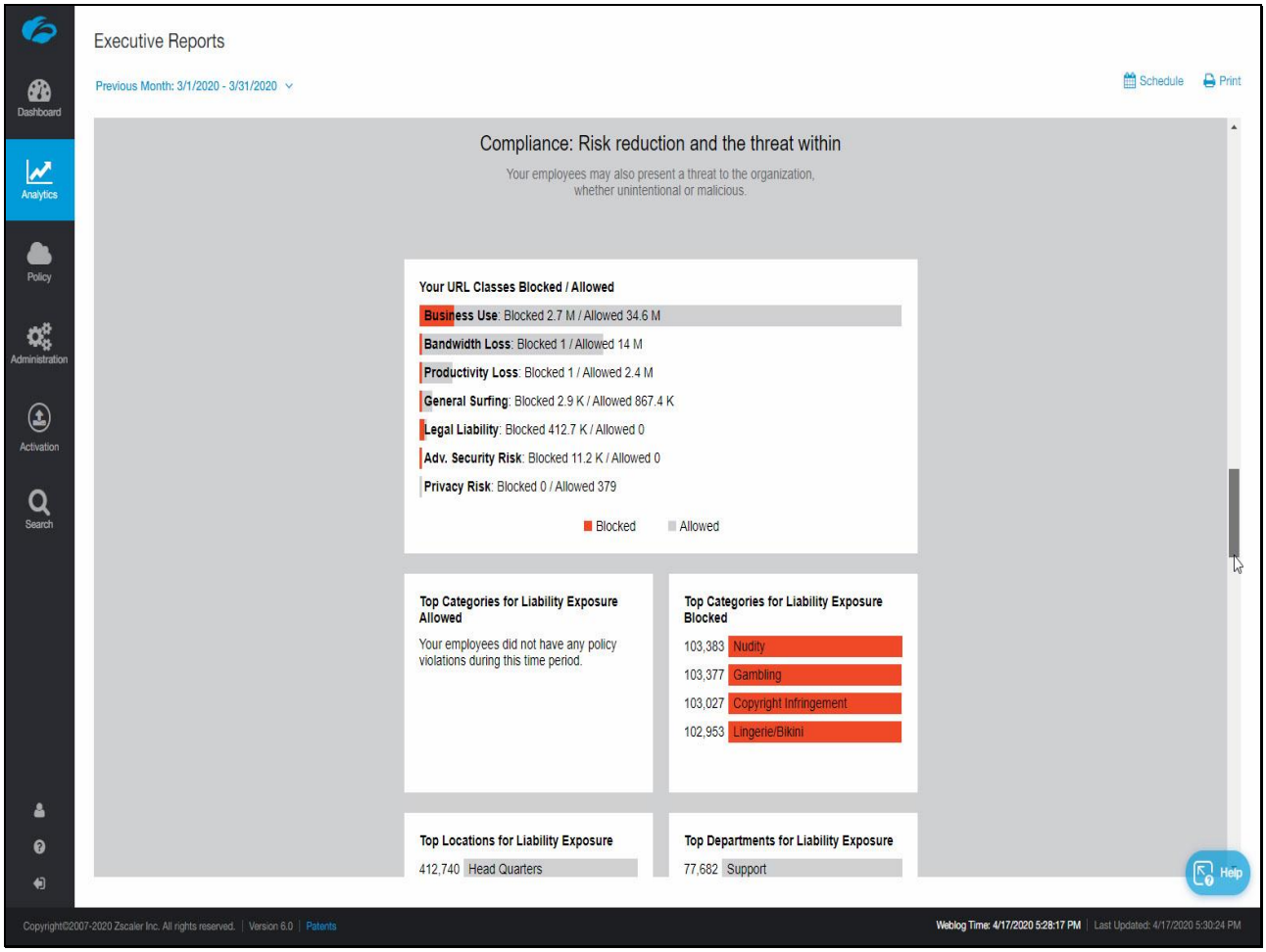
The compliance section shows what has been blocked or allowed by high level URL Classes based on your policies. This is then followed by a closer look at legal liability exposure by showing what is being allowed and what is being blocked as well as where this traffic is coming from by location and departments. Viewing your legal liability exposure helps your organization to understand employee behavior.

Slide 51 - Slide 51



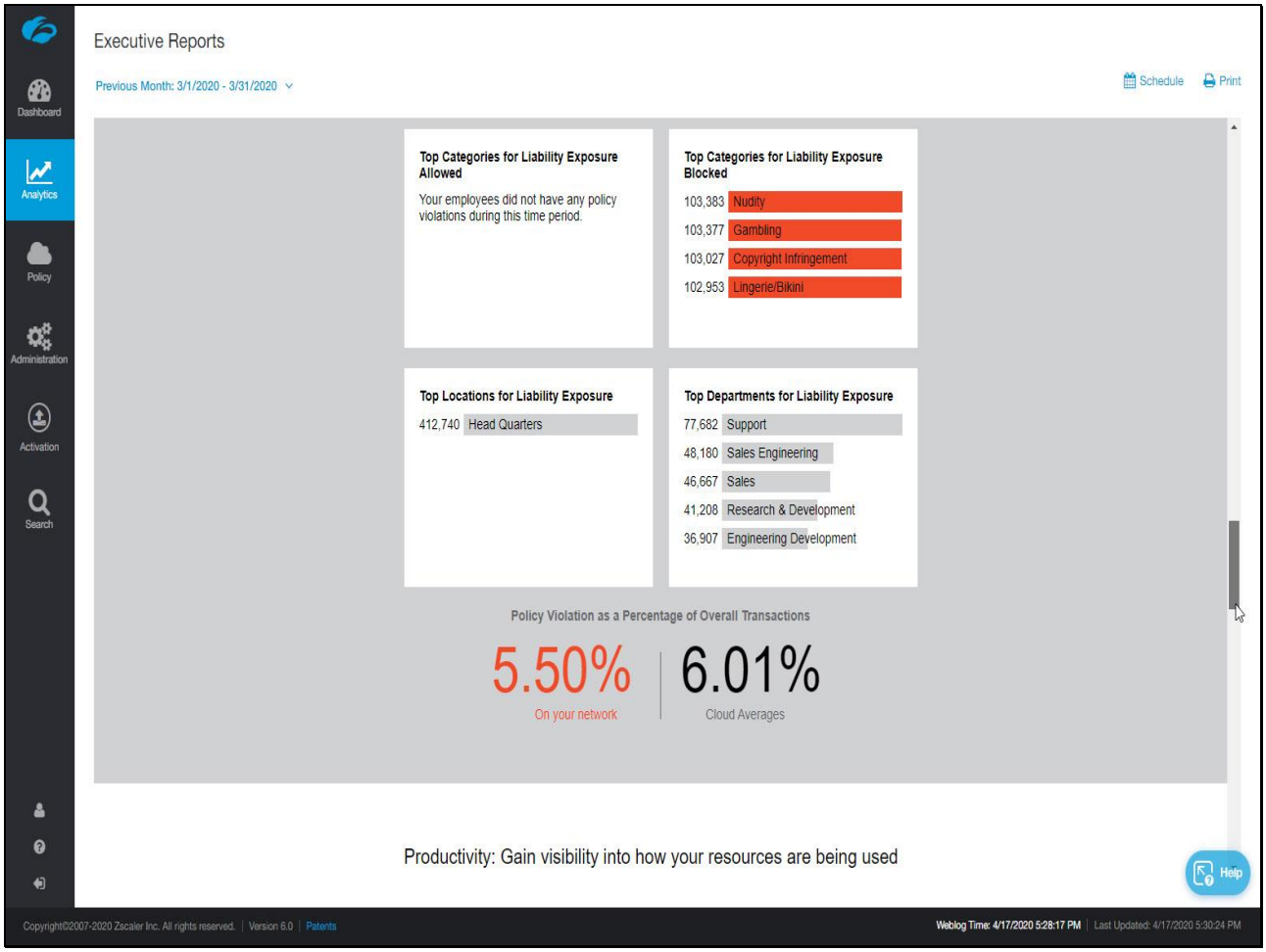
Slide notes

Slide 52 - Slide 52



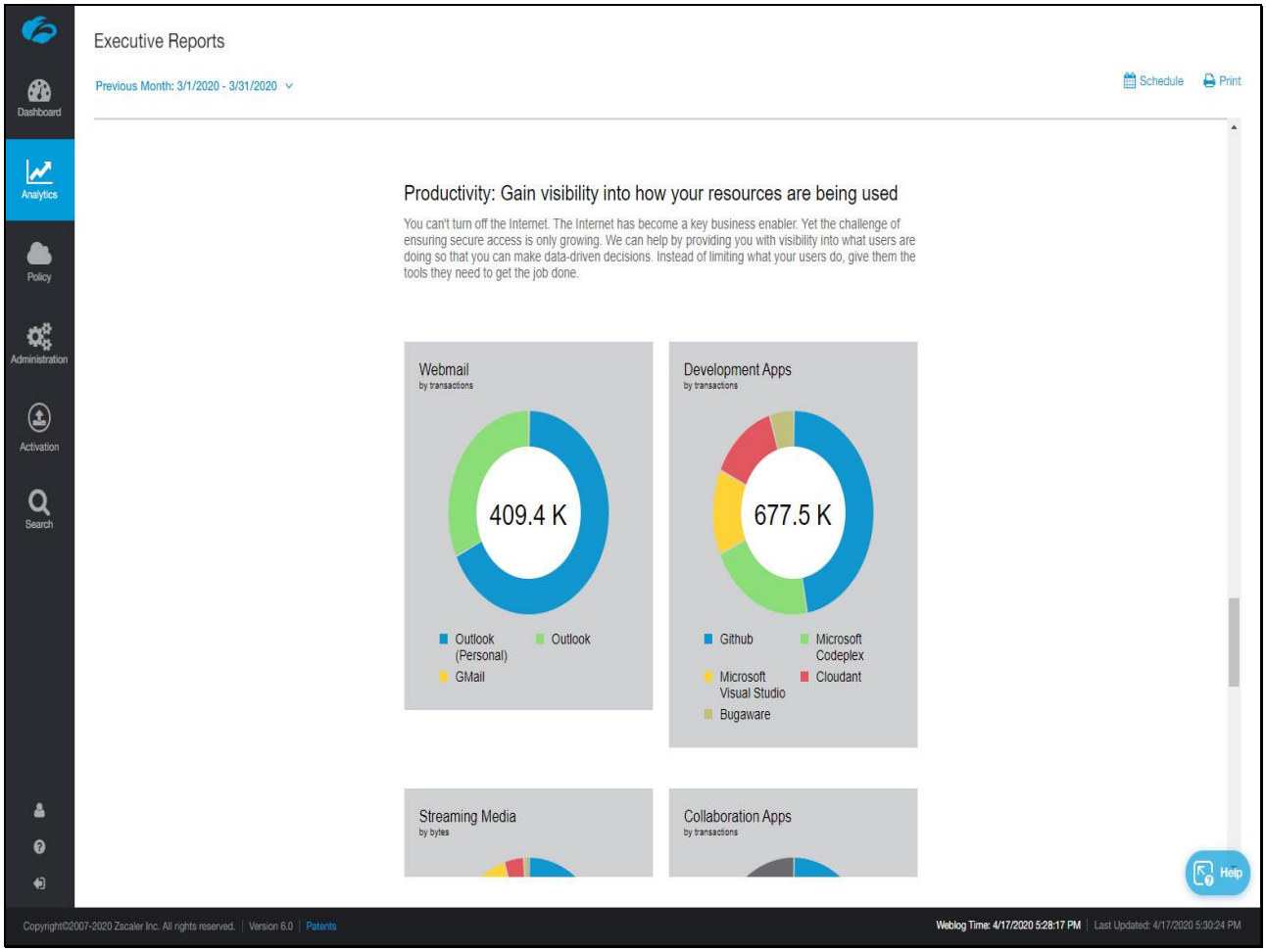
Slide notes

Slide 53 - Slide 53



Slide notes

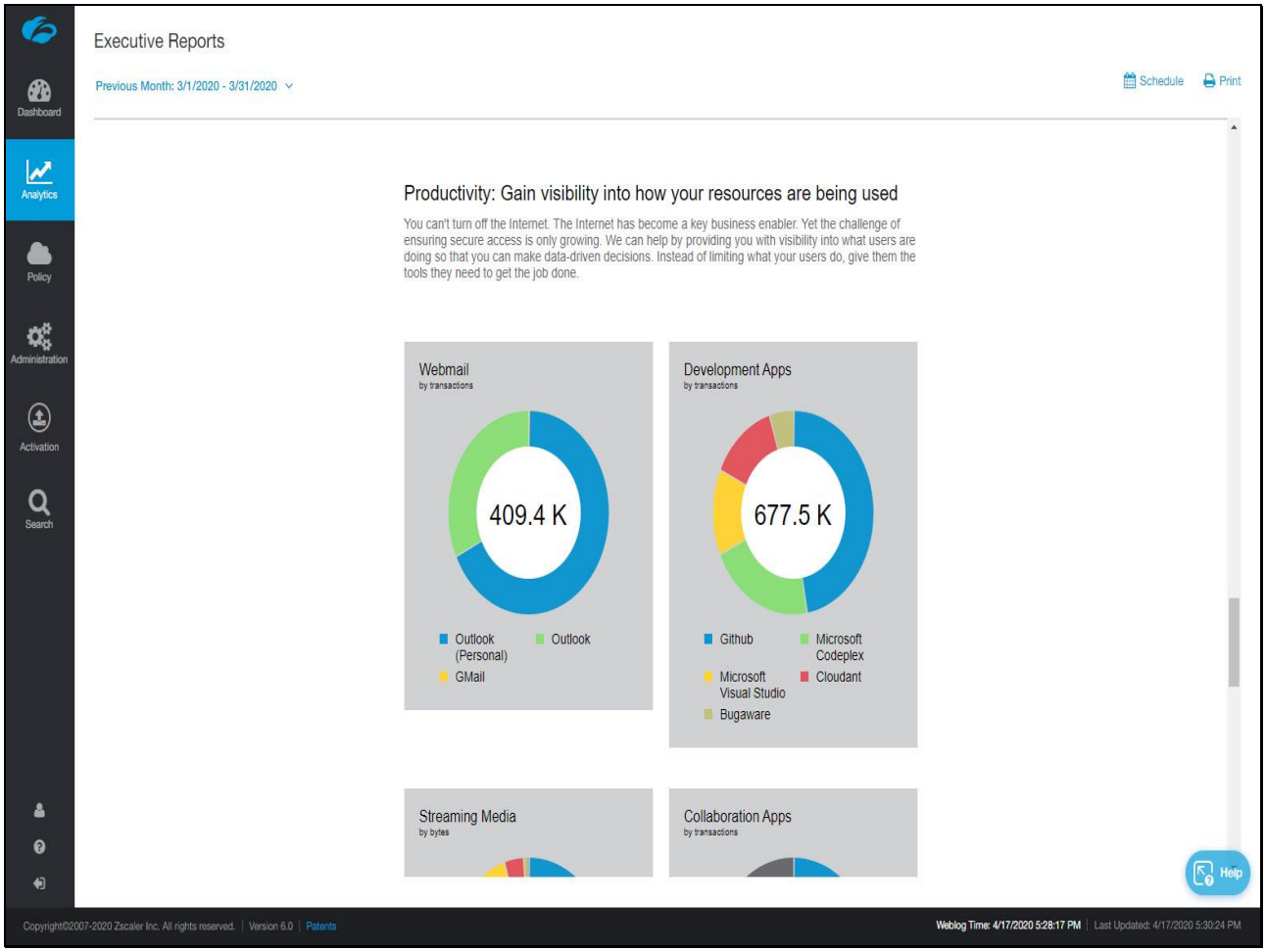
Slide 54 - Slide 54



Slide notes

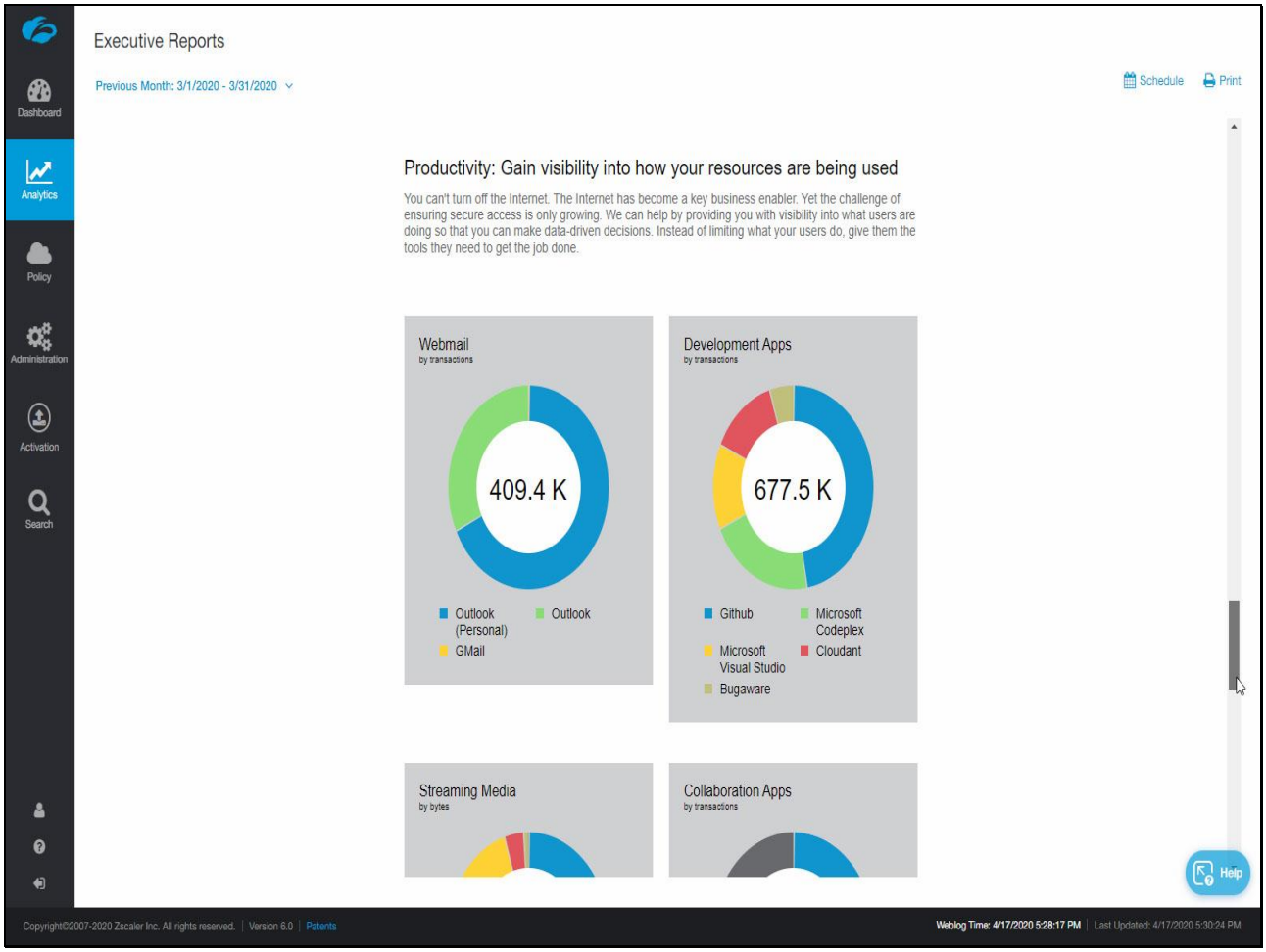
The productivity section shows the executives and Administrator where and what applications the users are spending their time on. With this understanding, you can determine if employee productivity is being impacted.

Slide 55 - Slide 55



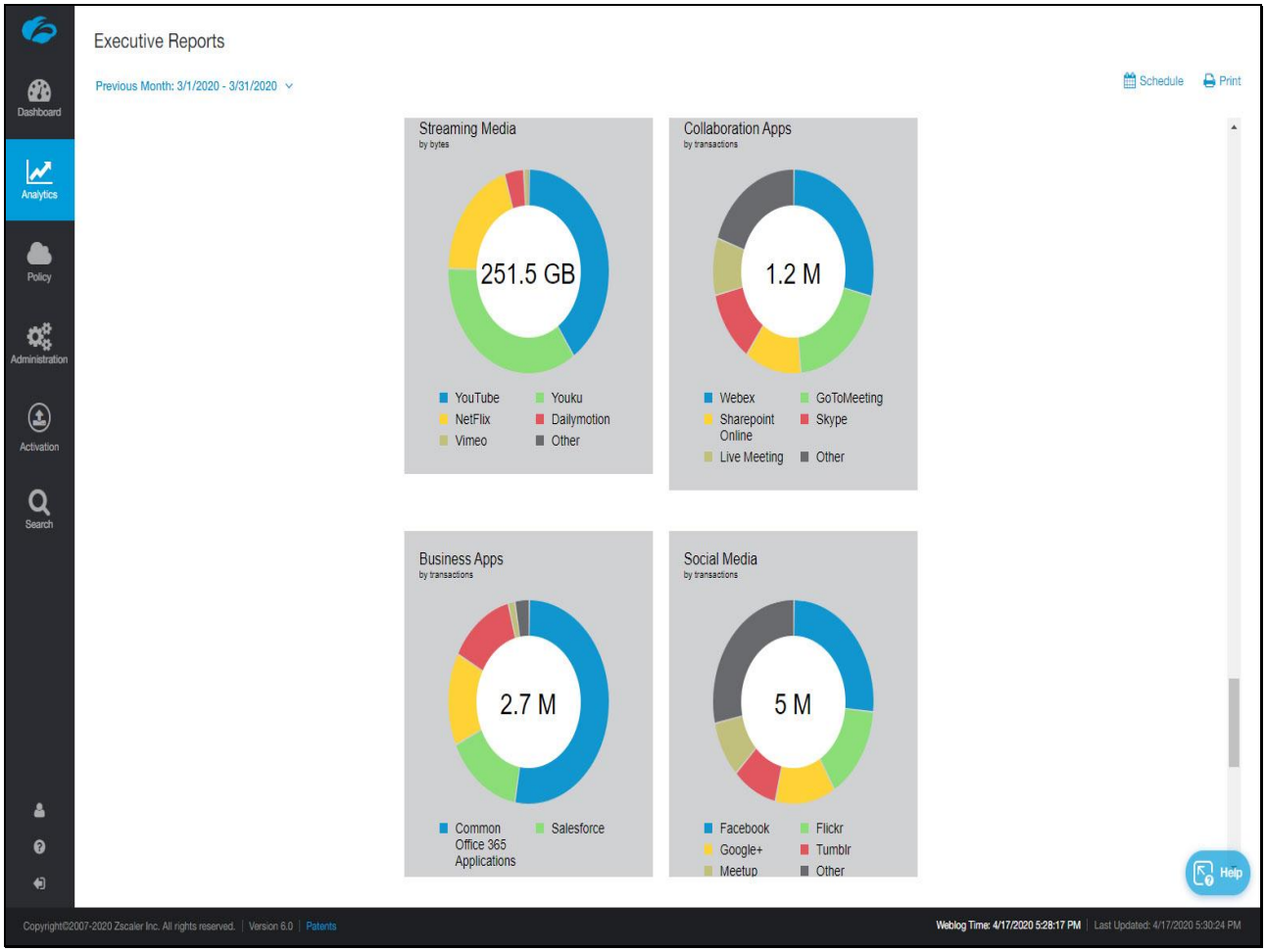
Slide notes

Slide 56 - Slide 56



Slide notes

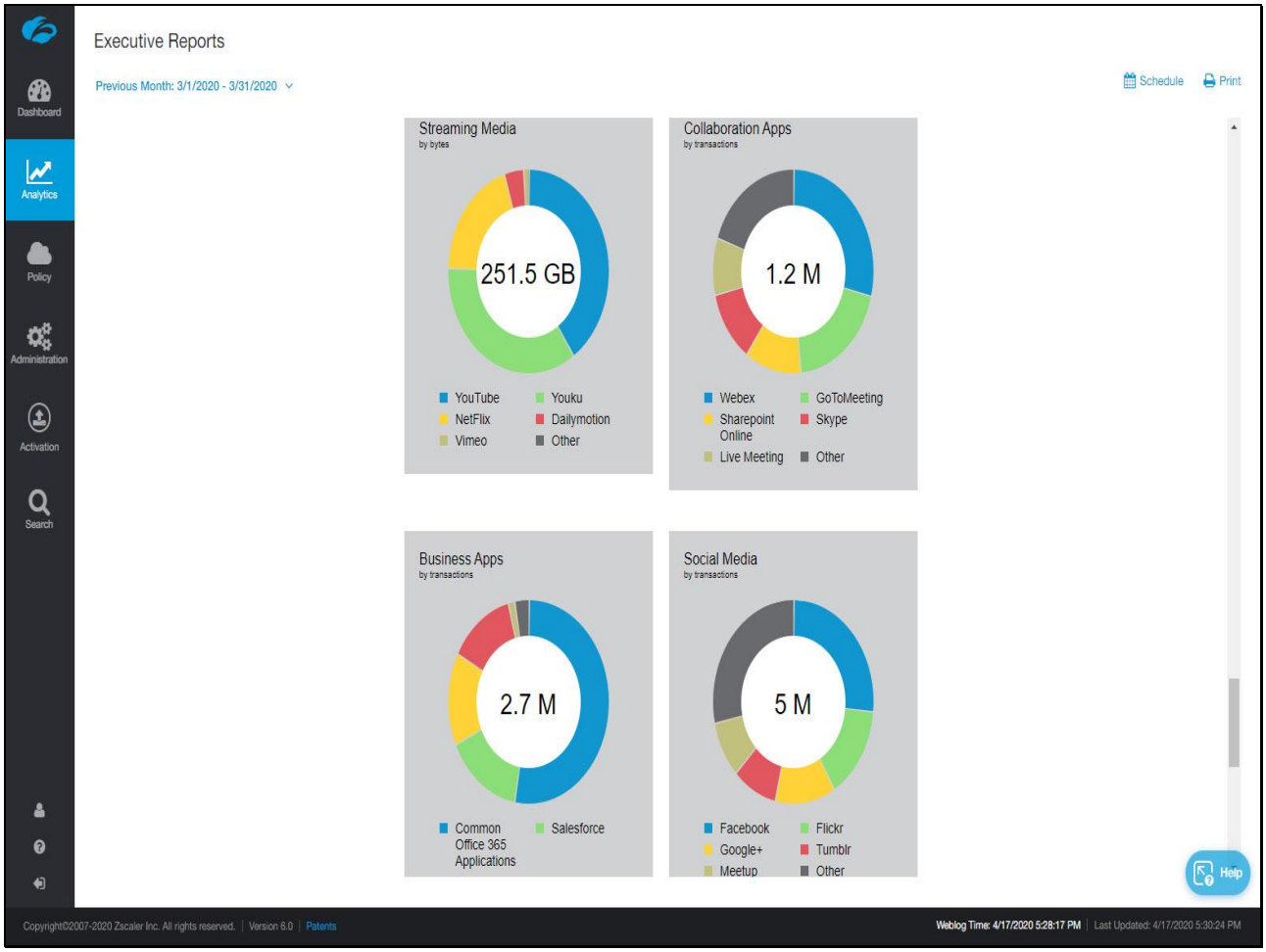
Slide 57 - Slide 57



Slide notes

If, for example, you see users spending a lot of time on Facebook, and your organization does not have a legitimate business use for Facebook you know there is an issue that needs to be addressed.

Slide 58 - Slide 58

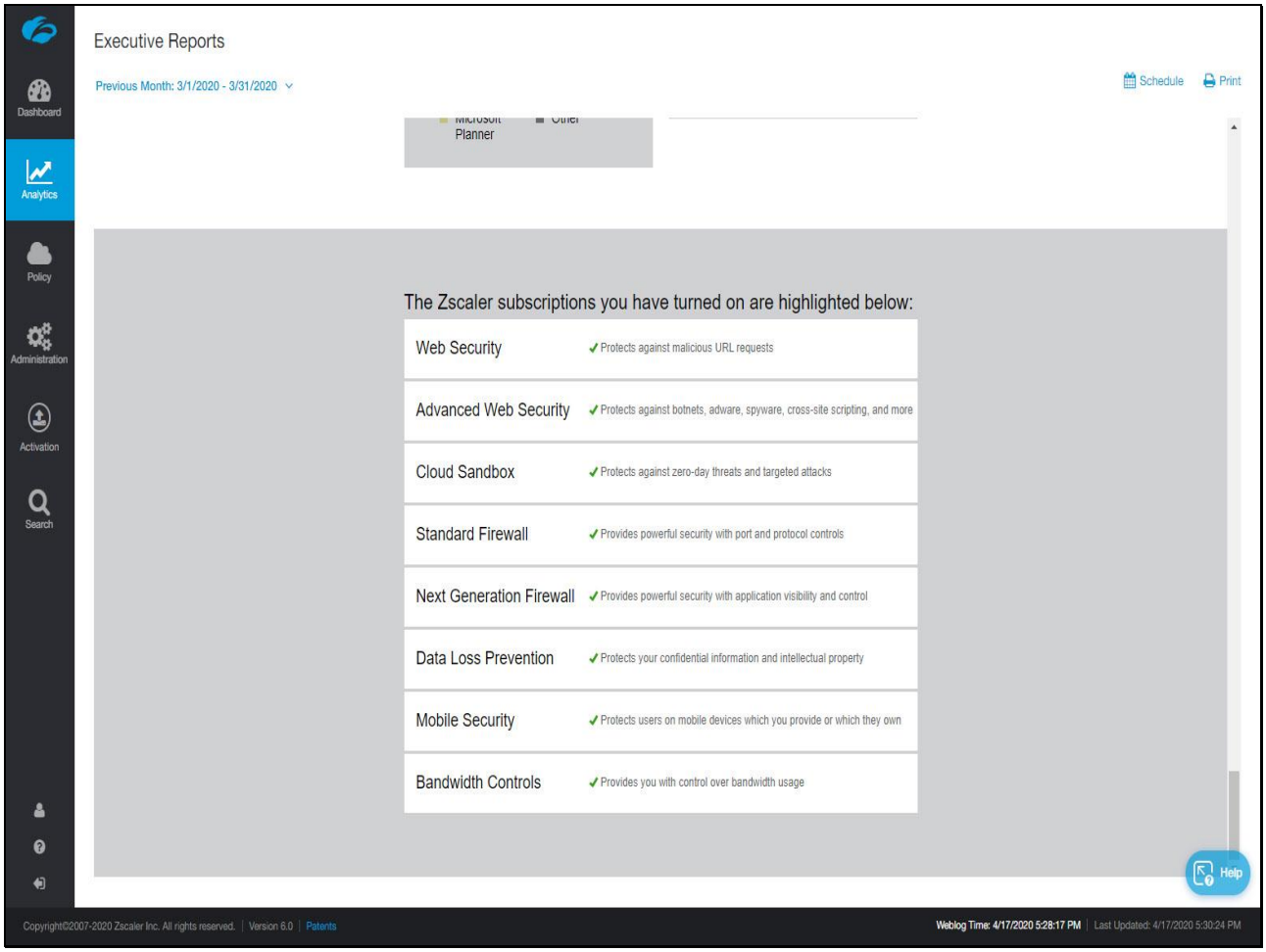


Slide notes

Slide 59 - Slide 59

Slide notes

Slide 60 - Slide 60



Slide notes

The last section on the Executive report shows what protections are enabled for your organization based on what features you subscribe to. Complete details on your subscription can be found in the Admin UI under Administration then Company profile; however, this view is much easier to understand.

Slide 61 -

Industry Peer Comparison Report

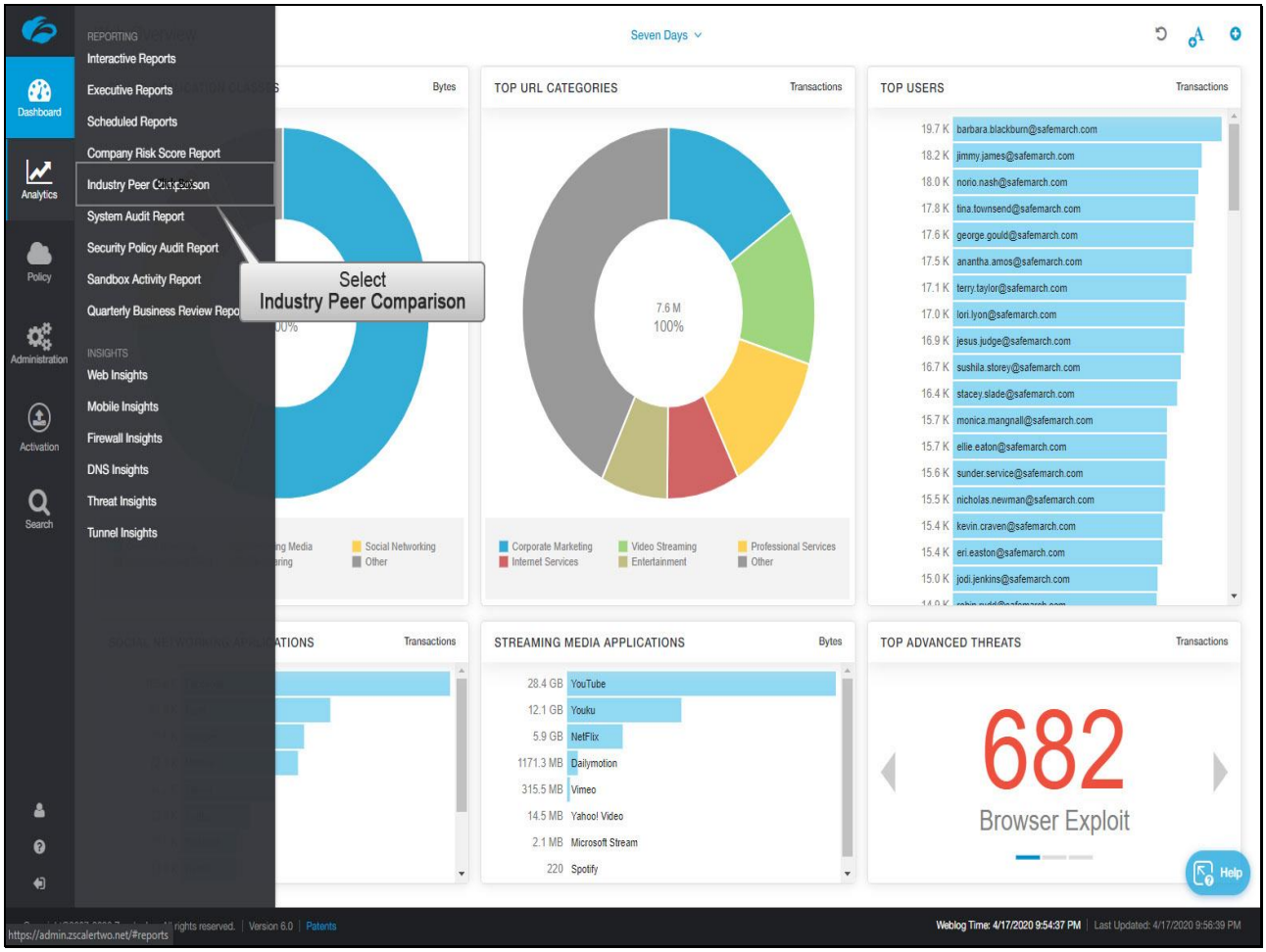
Slide notes

Slide 62 - Slide 62

Slide notes

As a new Zscaler Admin, after viewing the data in the Executive Report and understanding trends in your environment, you may be wondering if what you are seeing is normal or atypical. The next step is understanding how your organization is doing as compared to your peer organizations. Begin by clicking on **Analytics**.

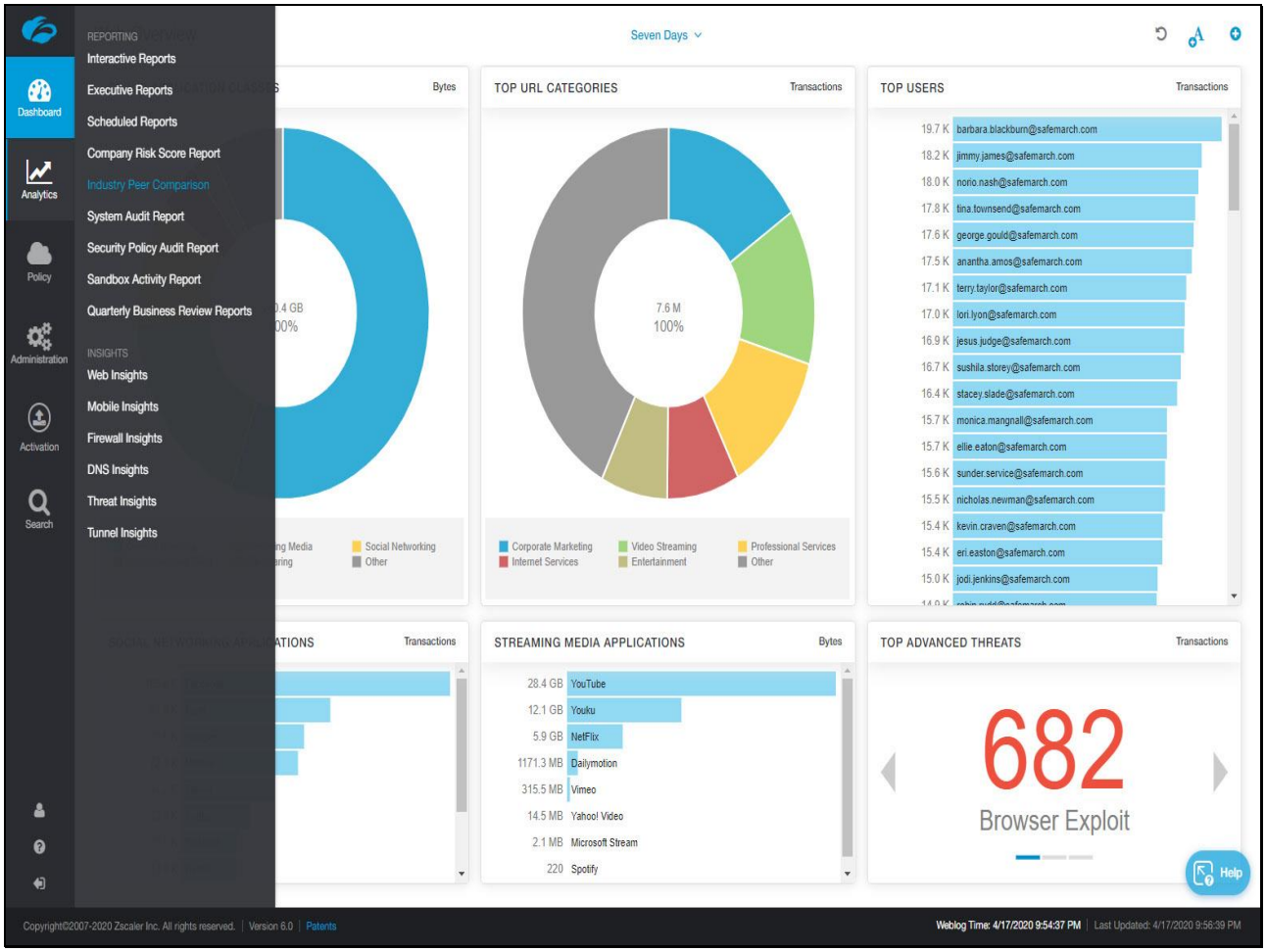
Slide 63 - Slide 63



Slide notes

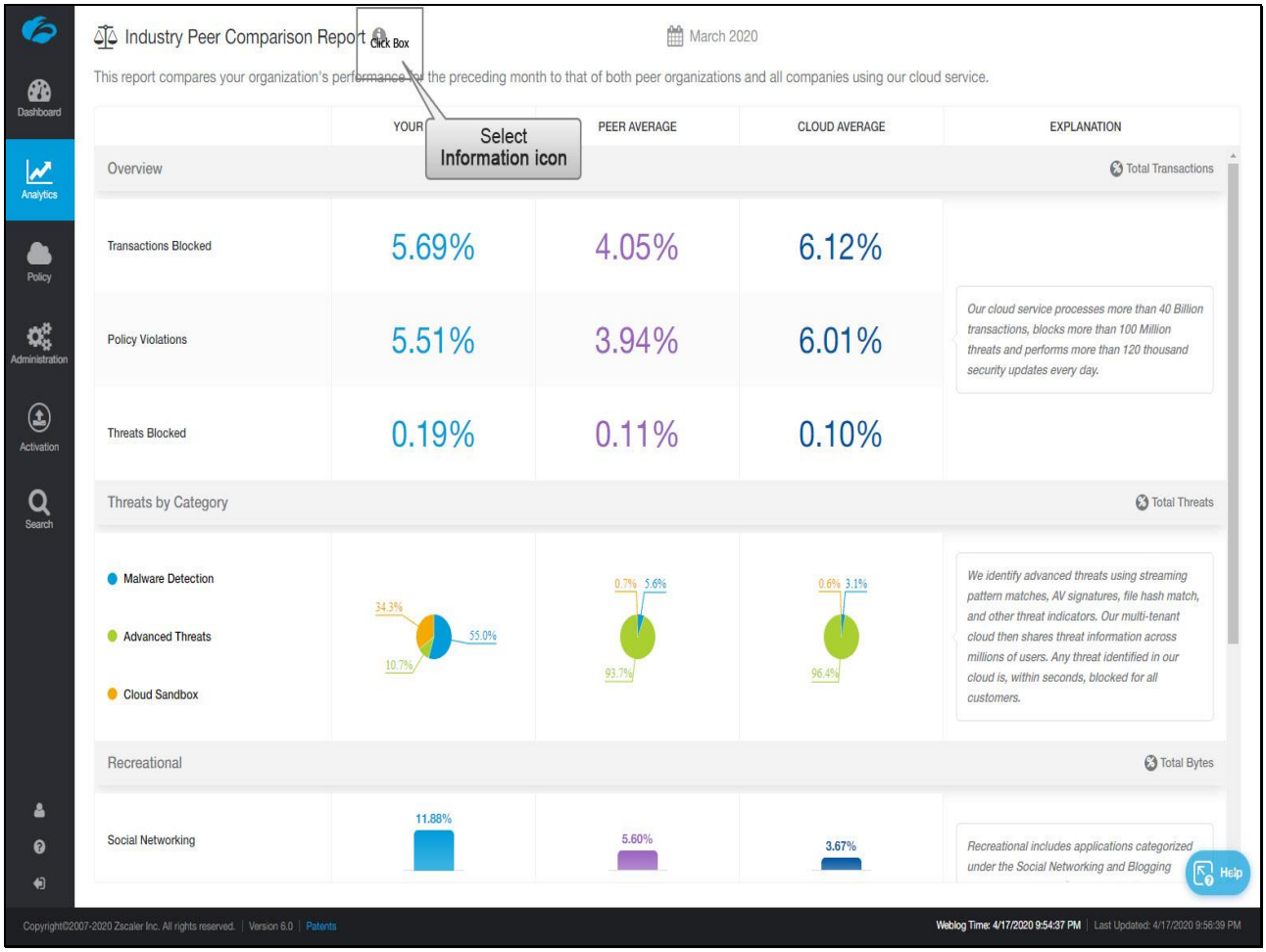
Then **Industry Peer Comparison.**

Slide 64 - Slide 64



Slide notes

Slide 65 - Slide 65

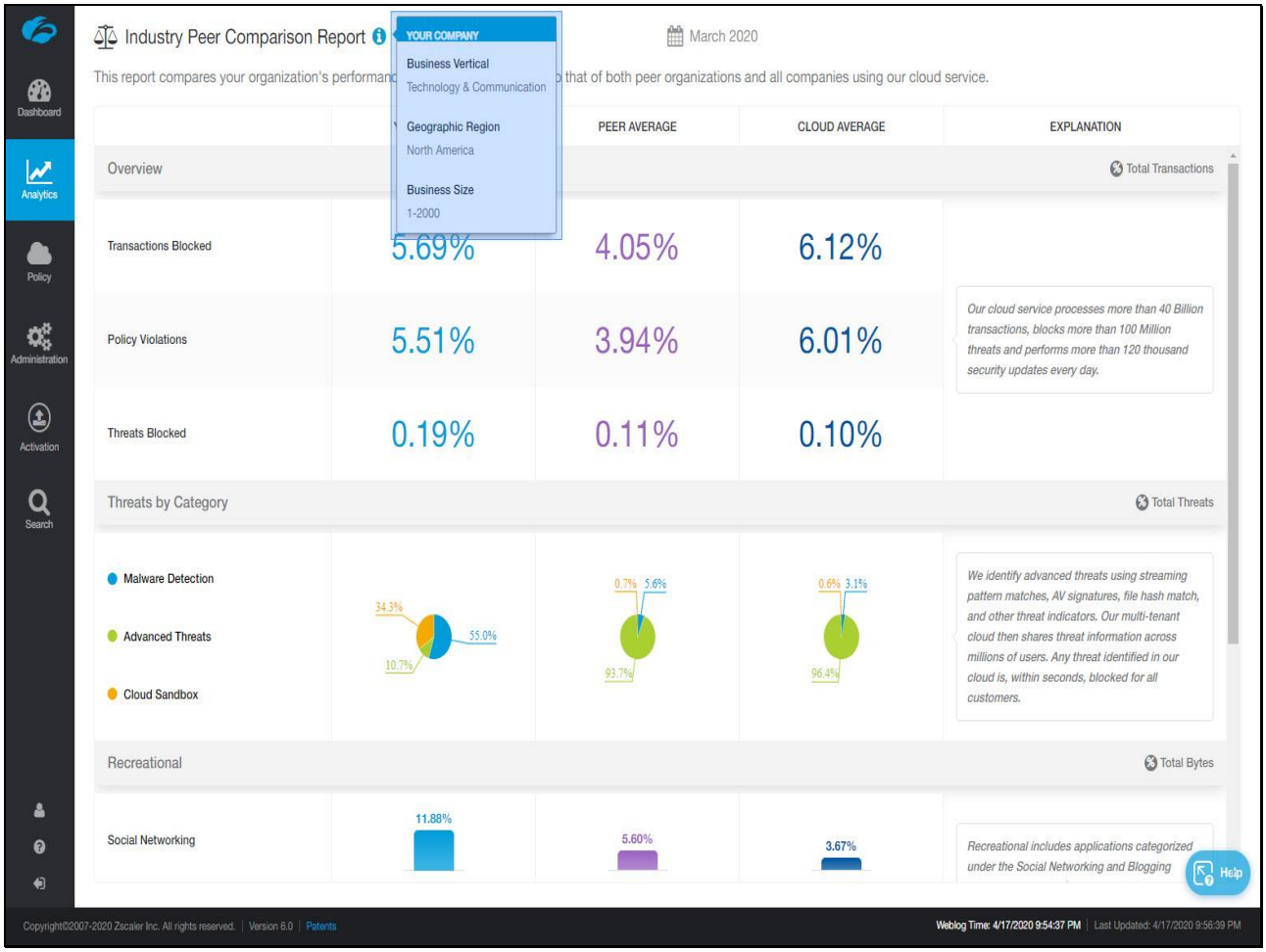


Slide notes

The Industry Peer Comparison Report compares your organization's performance and effectiveness for the preceding month to that of both peer organizations and all companies using our cloud service. Peers are chosen based on business vertical, geographic region, and business size. Viewing this report helps you to quickly understand if you are seeing unusual levels of activity, as compared to your peers, and if so, in what areas.

When you signed up as a Zscaler customer your account was classified into the appropriate business vertical and size classification. You can see your organizations assigned vertical, Geographic Region, and Business Size, or number of employees by clicking on the **"Information Icon"** near the upper left corner.

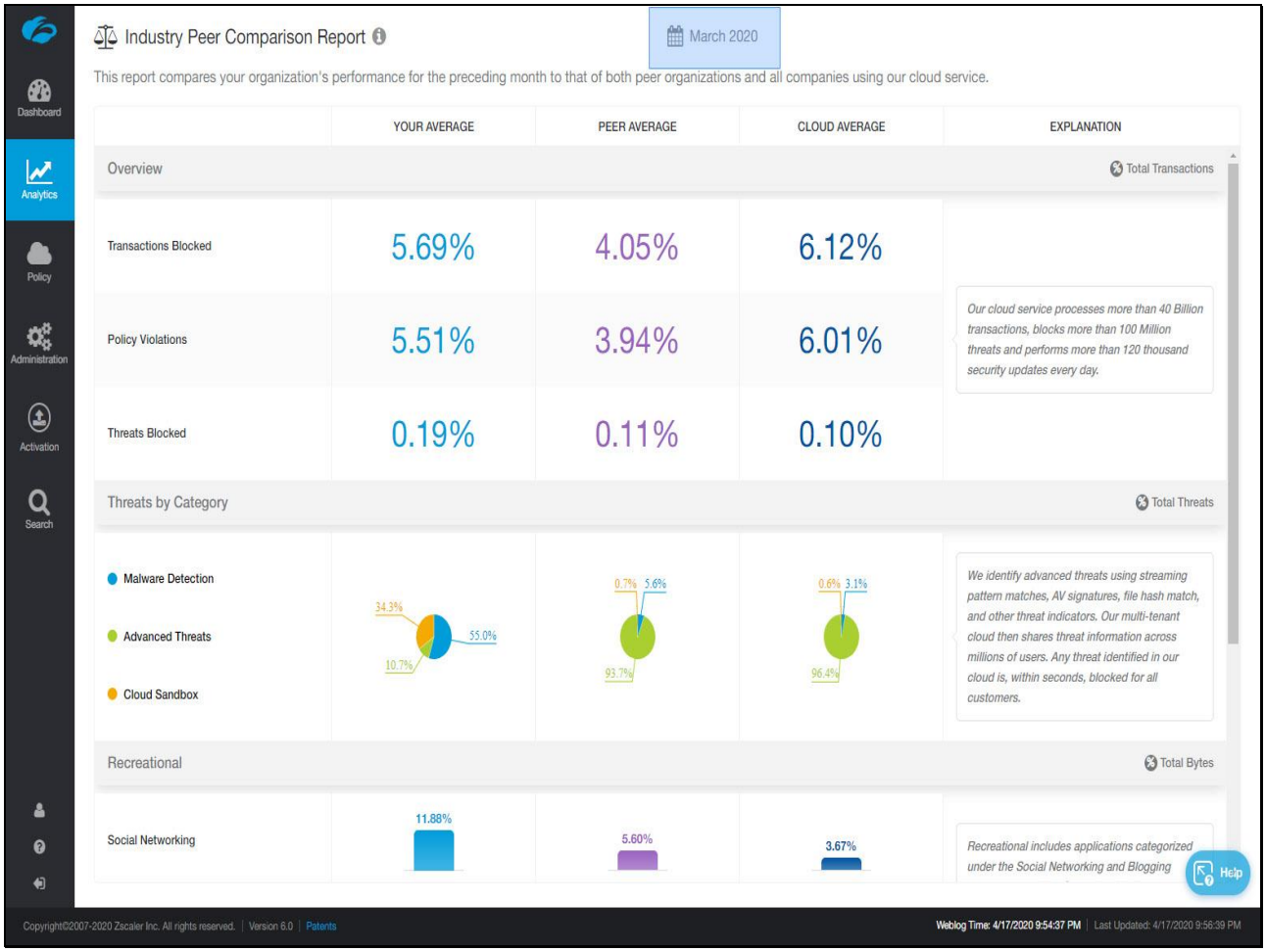
Slide 66 - Slide 66



Slide notes

These values determine who your organization is compared to under the “Peer” column. Your peers are similar customers on the Zscaler cloud. The Cloud Average looks at all customers across all Zscaler clouds.

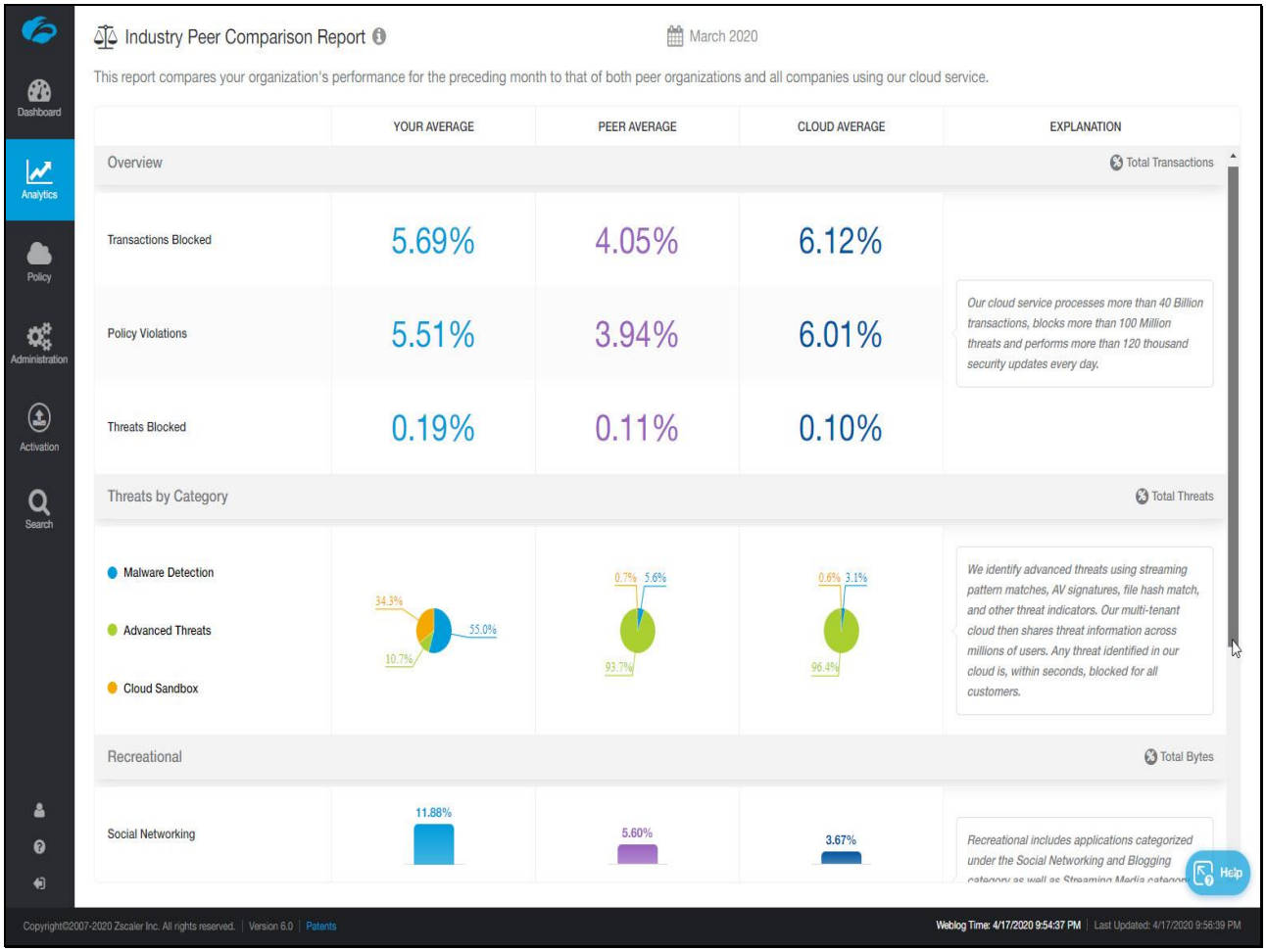
Slide 67 - Slide 67



Slide notes

This report is automatically generated monthly on first day of the month for the preceding month as observed near the top center of the screen. For example, on the first day of April 2020 the report was generated for the month of March.

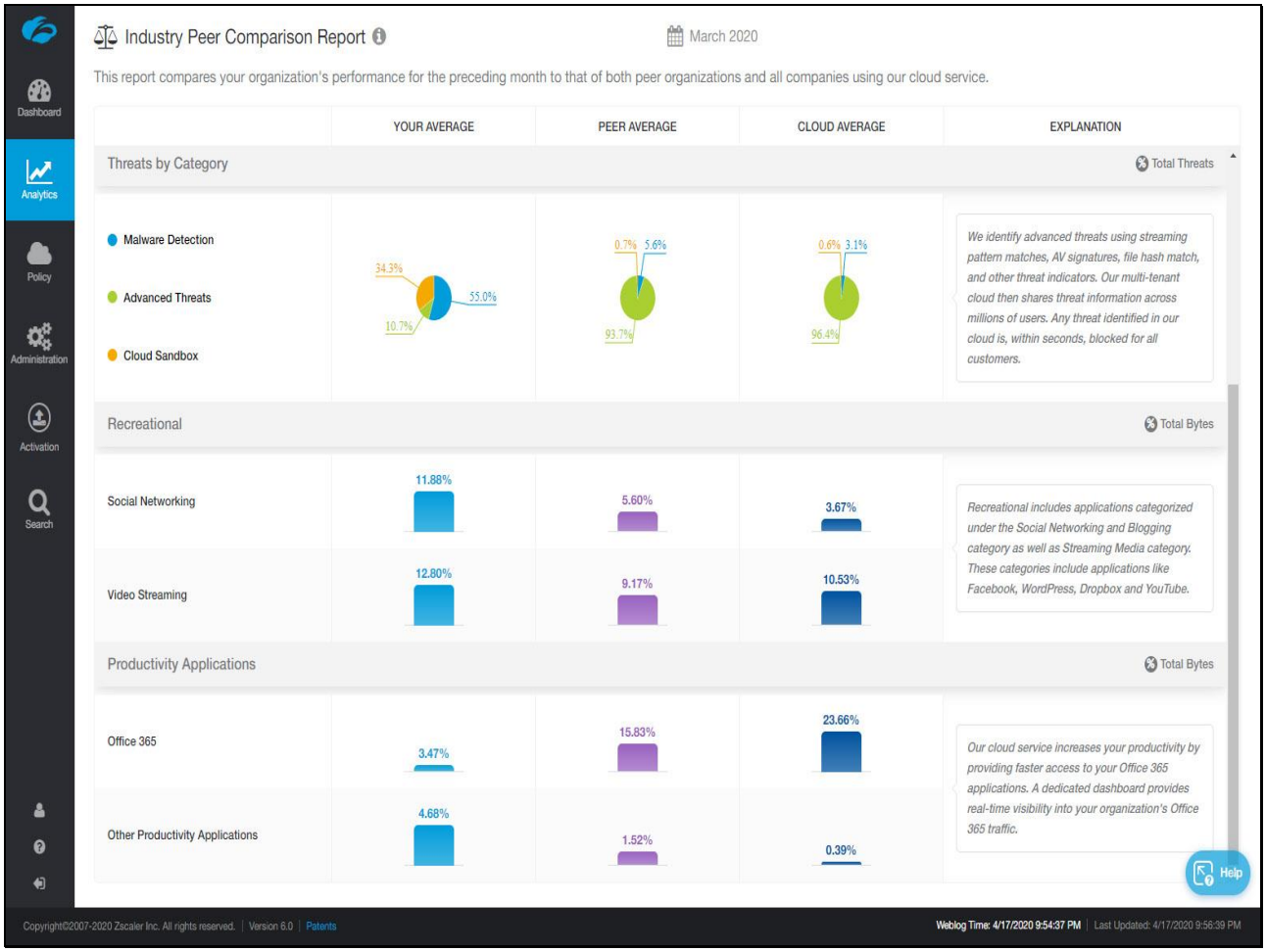
Slide 68 - Slide 68



Slide notes

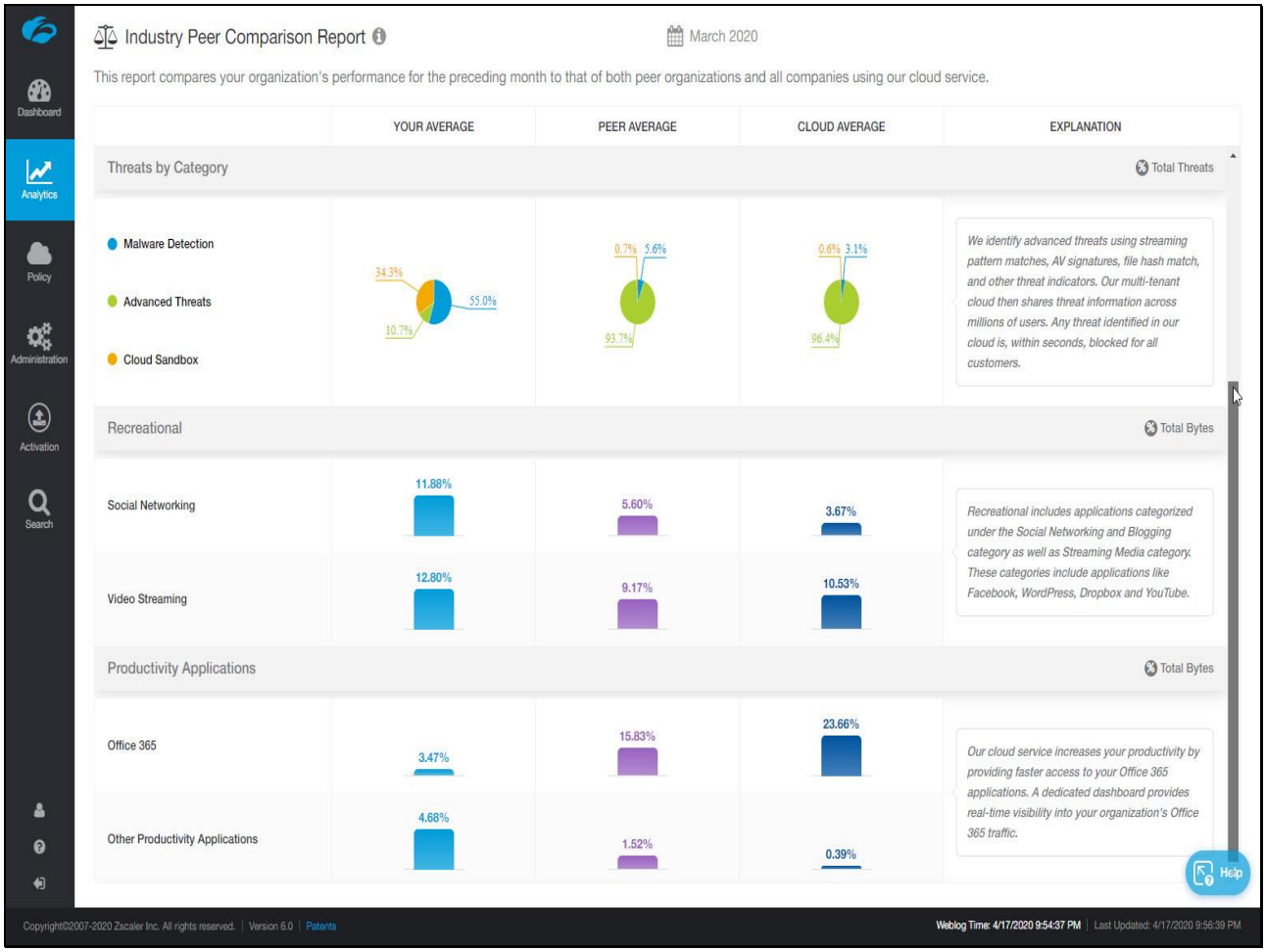
The report is broken down by overall traffic, threats by category, recreational applications, and productivity applications.

Slide 69 - Slide 69



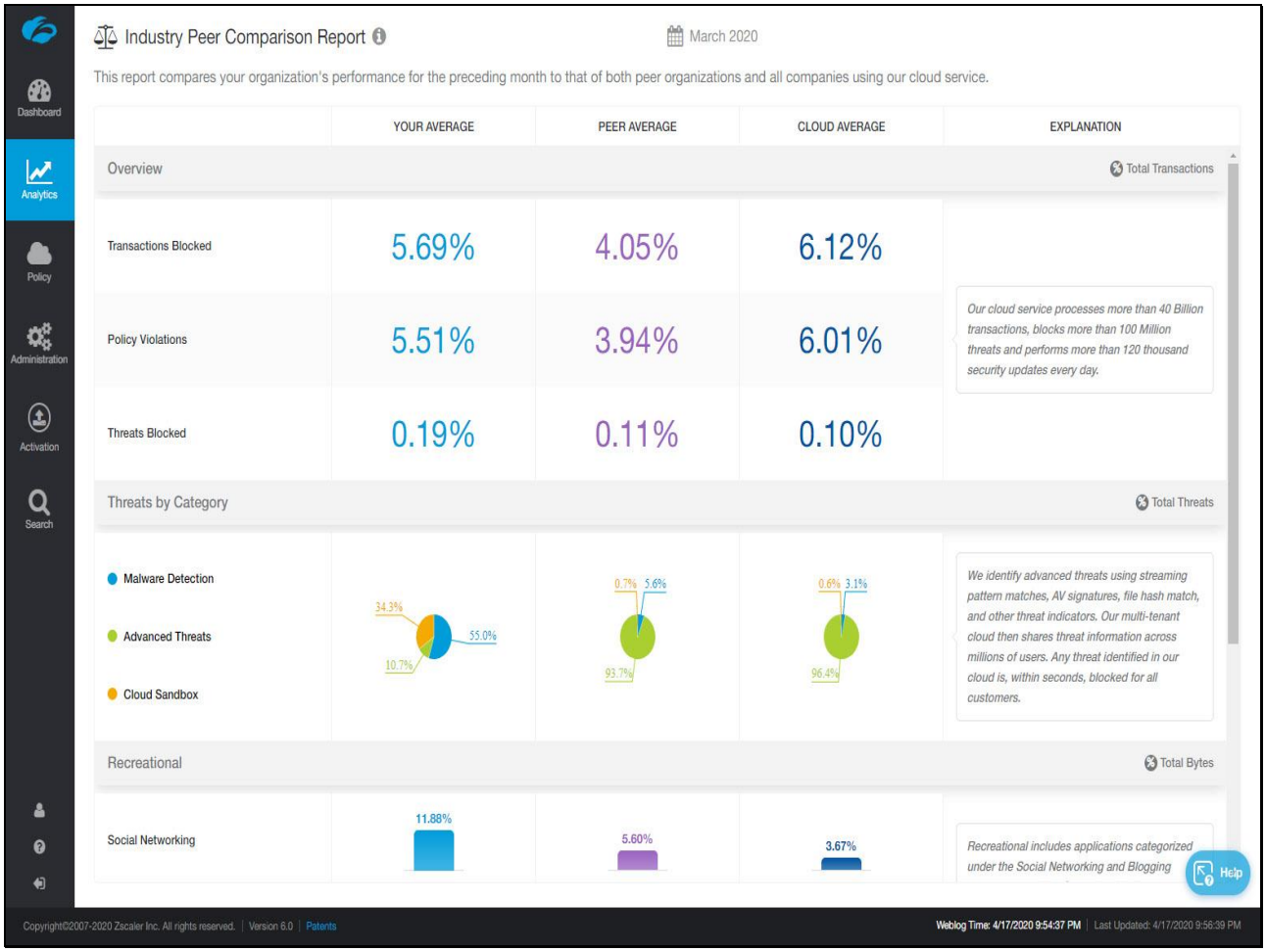
Slide notes

Slide 70 - Slide 70



Slide notes

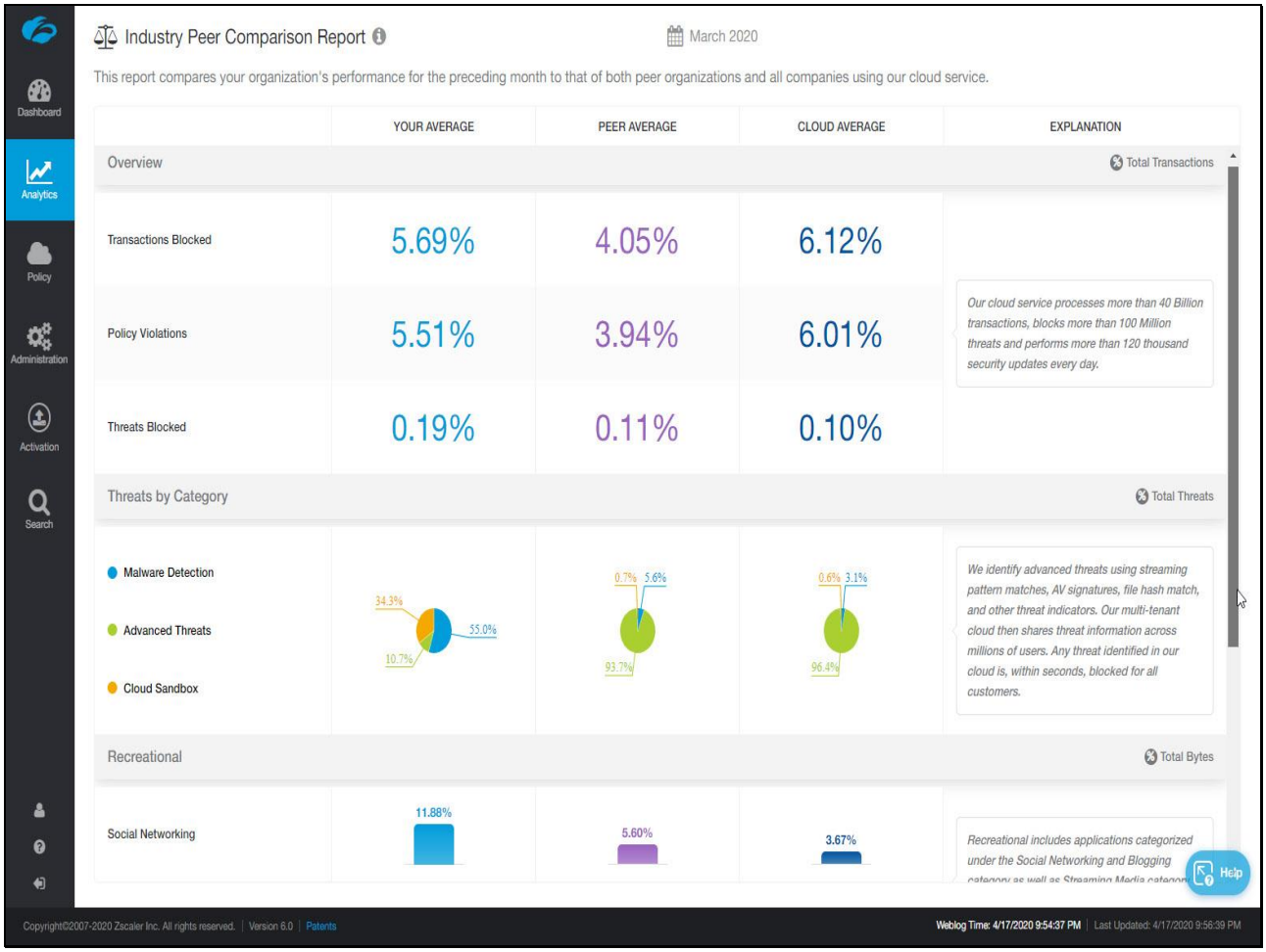
Slide 71 - Slide 71



Slide notes

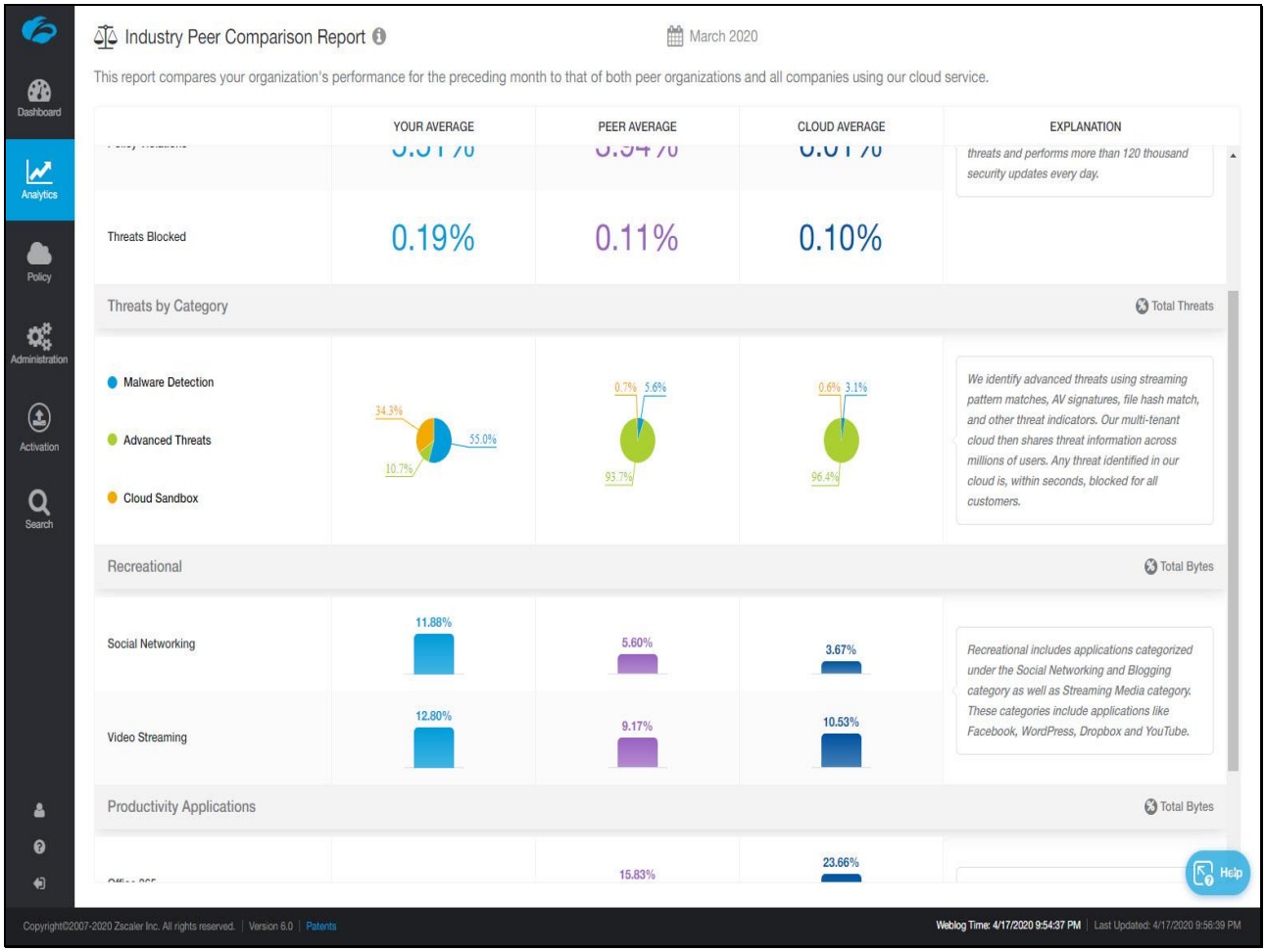
In this case, you can see that our averages are slightly worse as compared to our peers but better than the cloud average.

Slide 72 - Slide 72



Slide notes

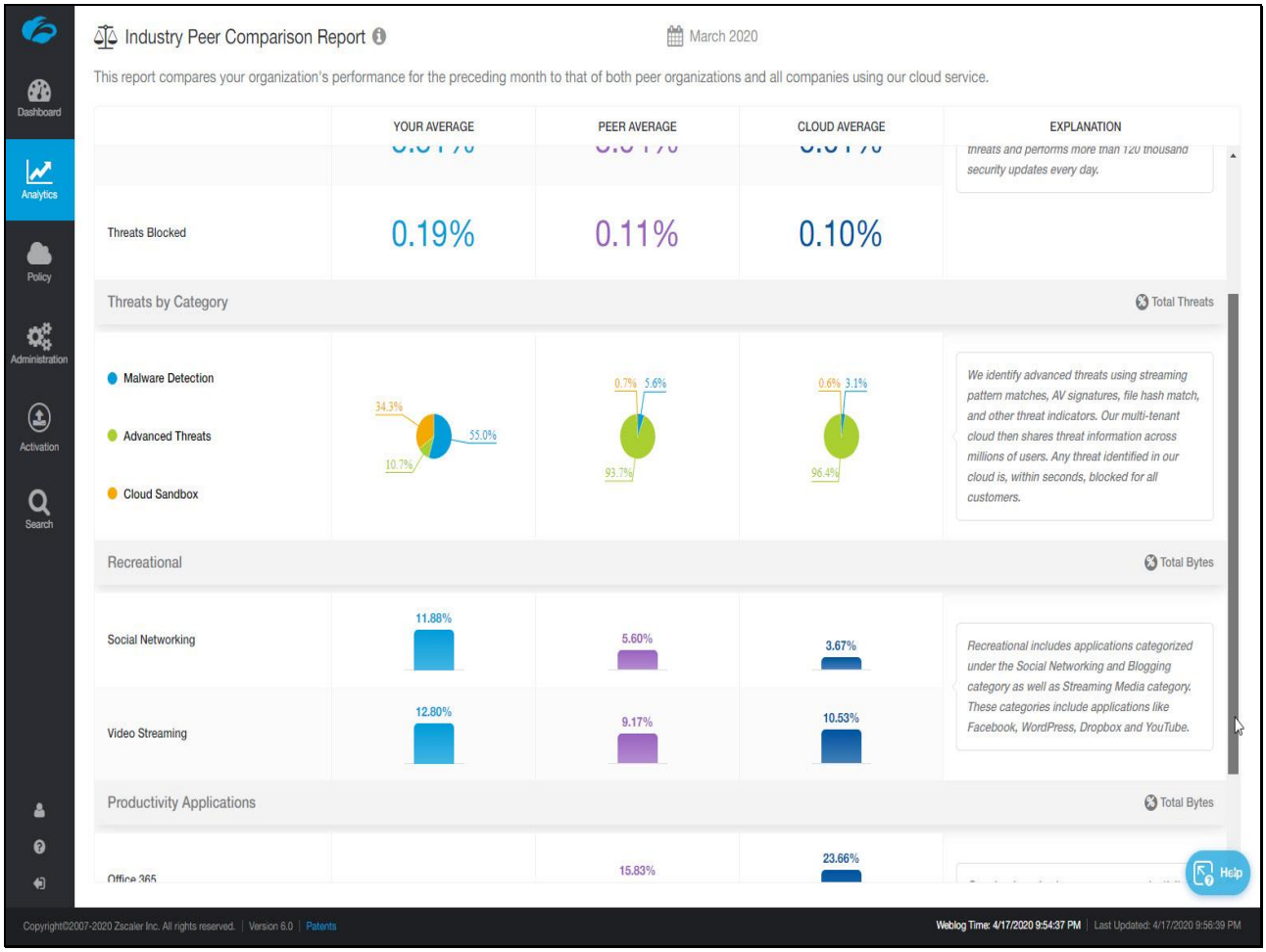
Slide 73 - Slide 73



Slide notes

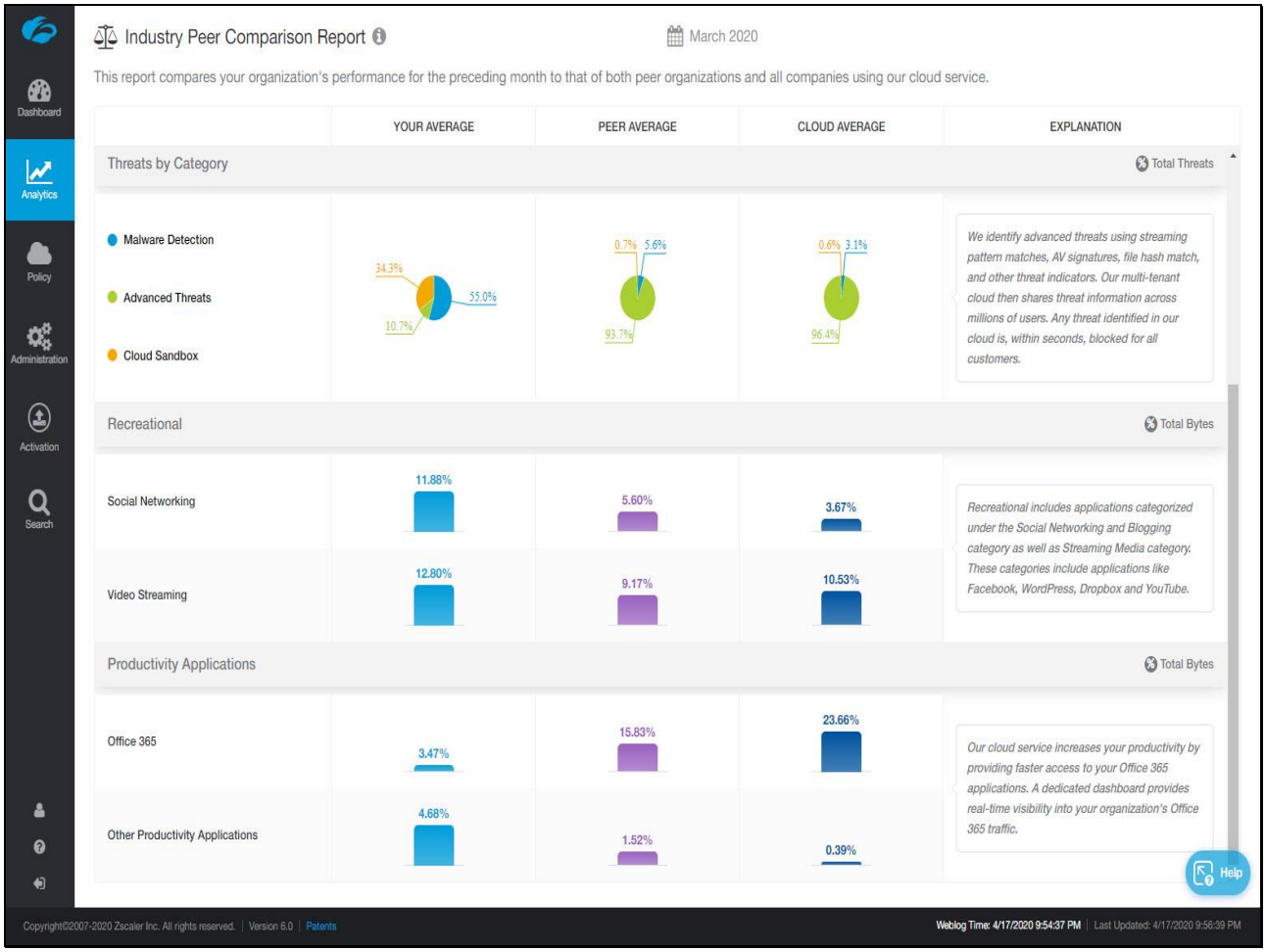
Moving down to “Threats by Category” we see that, of the threats blocked, 55% of those threats were malware and 11% were Advanced Threats. When compared to my peers, and the cloud averages, we see that the incidence of Malware we saw were significantly higher than my peers or the cloud. This should lead to further investigation under Analytics.

Slide 74 - Slide 74



Slide notes

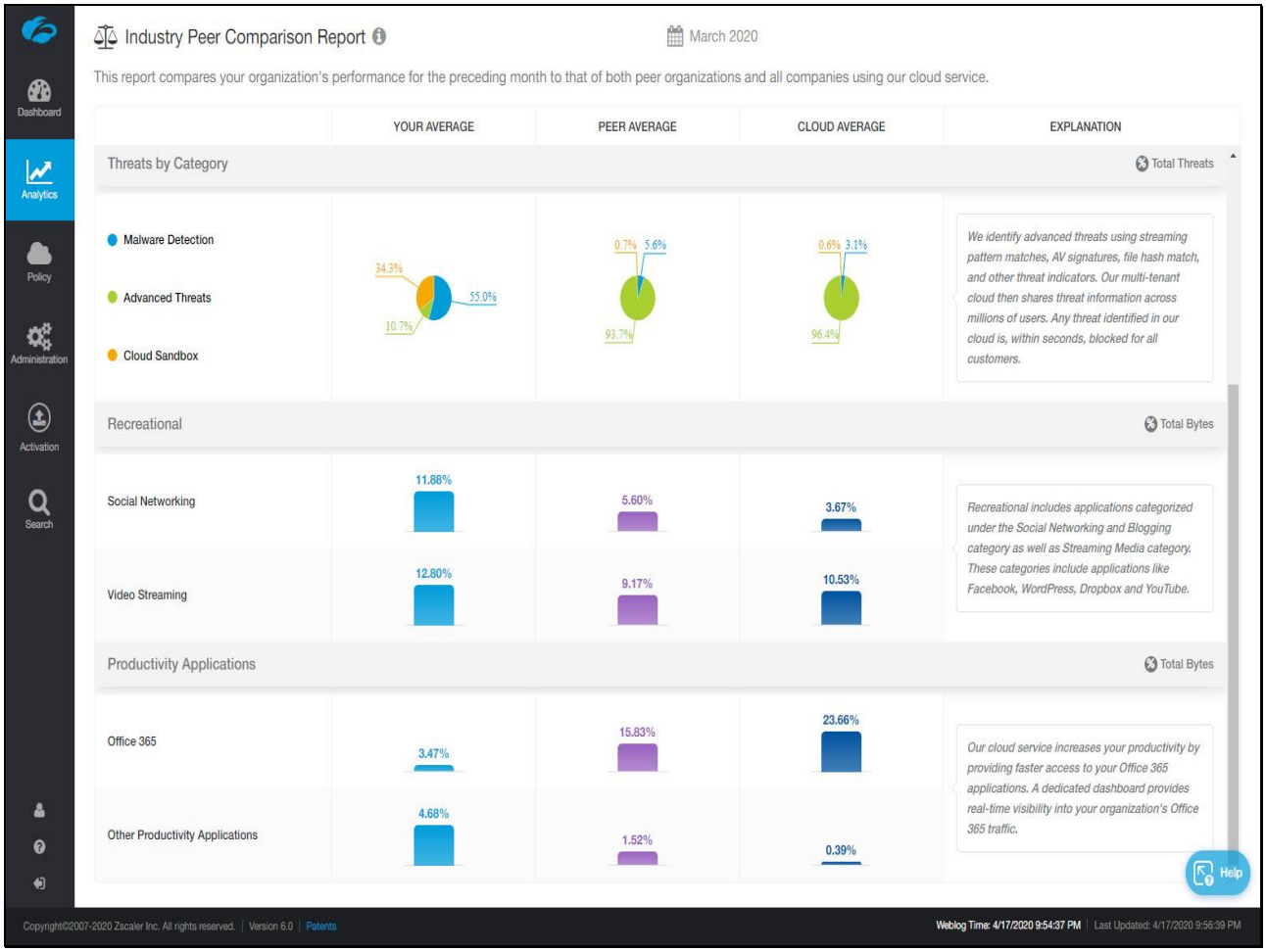
Slide 75 - Slide 75



Slide notes

Moving down to “Recreational” we see that our employees are spending more time using social networking applications and video streaming applications then our peers providing an indicator of user productivity.

Slide 76 - Slide 76



Slide notes

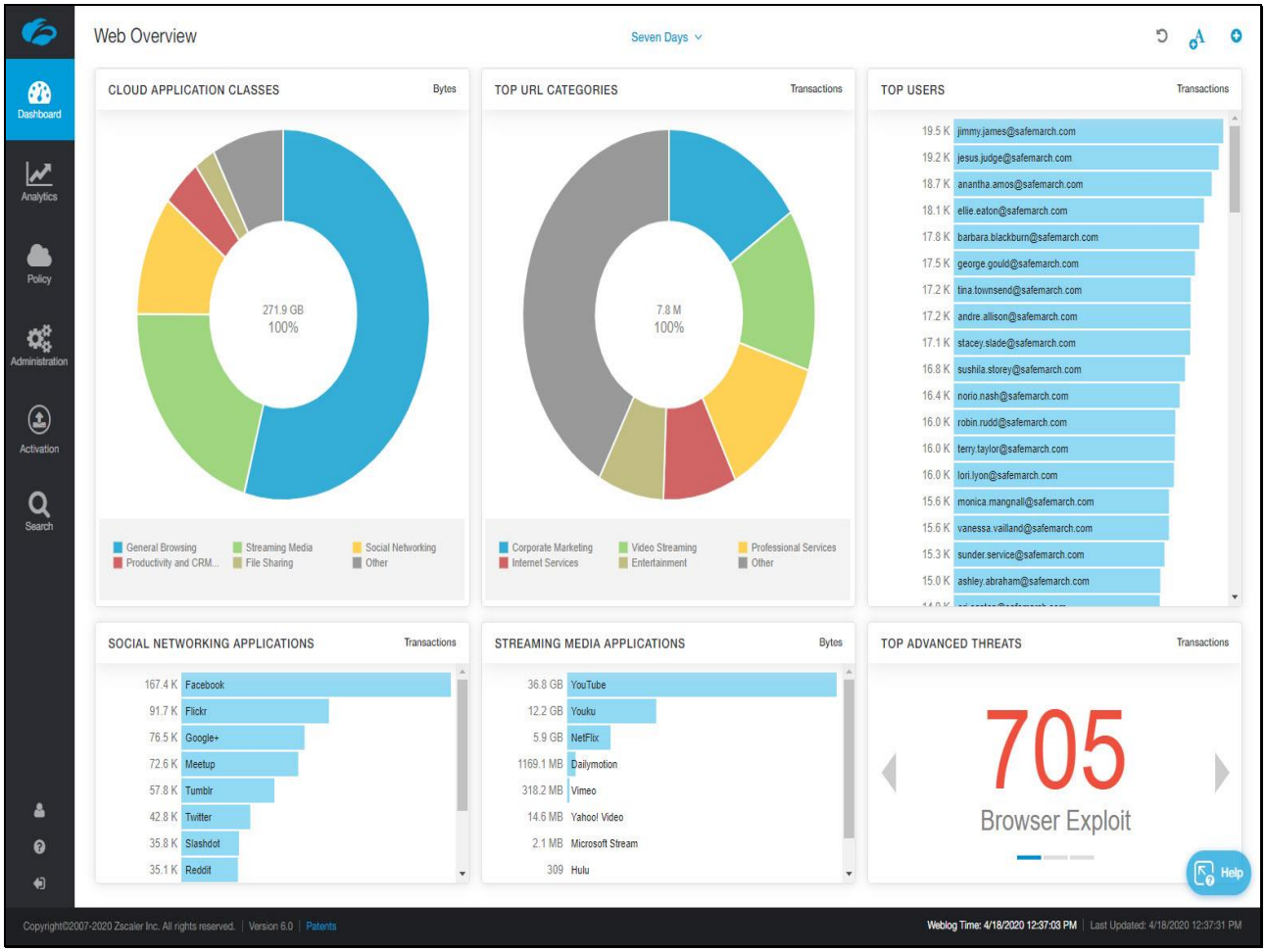
Last, we see that our organization is making use of productivity applications such as Office365 but not as much as similar organizations.

Slide 77 - Problem tracking using the Dashboard and Reporting

Slide notes

Let’s now look at using information presented in the dashboard to drill into traffic flows, find what may be an issue, and look at the results of our remediation put in place to solve the problem we found.

Slide 78 - Slide 78



Slide notes

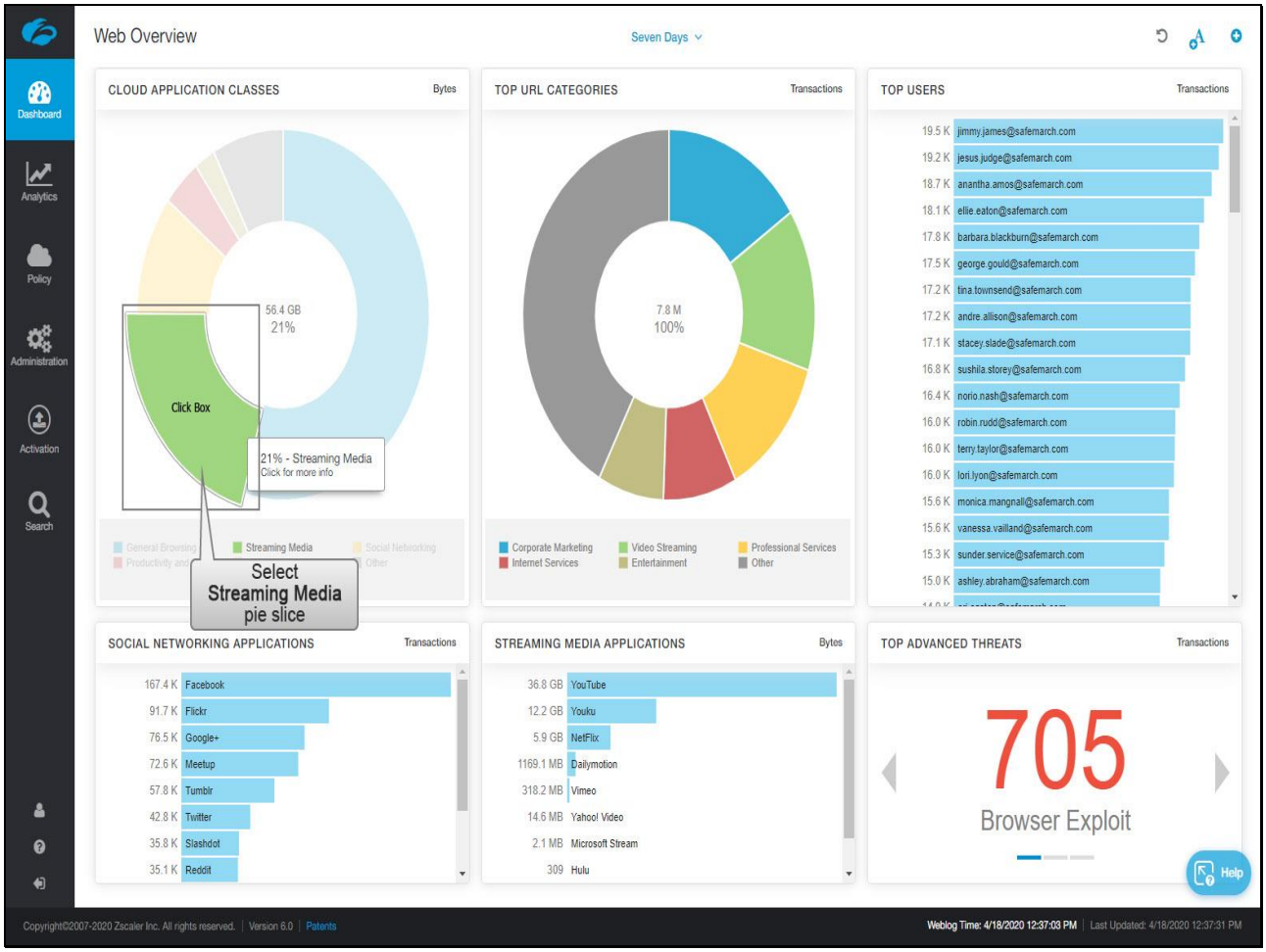
Let's assume that you, as the Admin, believe there is a bandwidth consumption issue at one, or more, of your sites. You can use the dashboard to quickly assess what type of traffic, in terms or URL categories or Cloud applications, for example, is flowing through your network.

Slide 79 - Slide 79

Slide notes

As you move your mouse around the pie chart you see that the “Streaming Media” is consuming a lot of bandwidth as seen under both URL Categories and Cloud application classes.

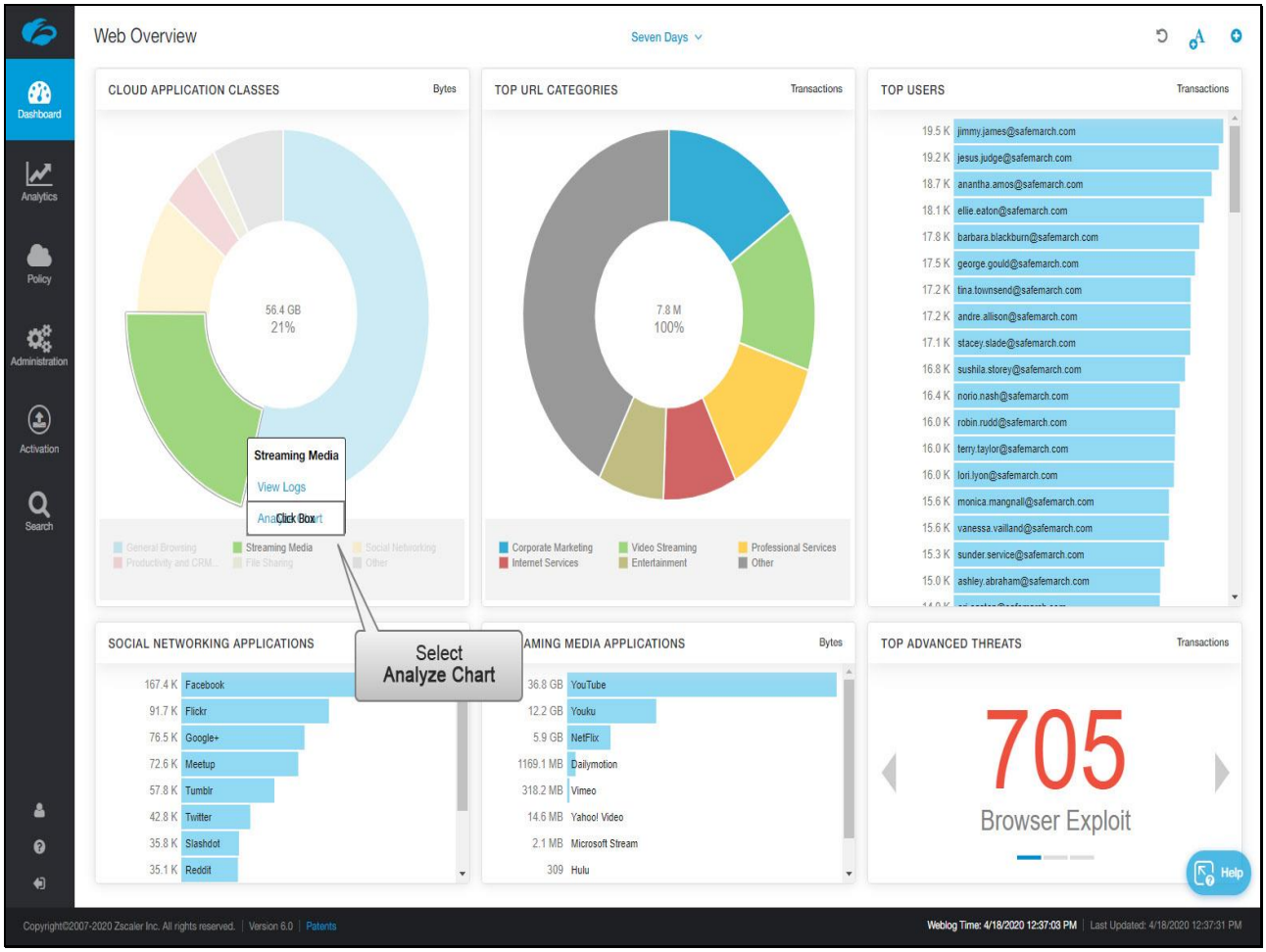
Slide 80 - Slide 80



Slide notes

Click in the **Streaming Media** pie slice under Cloud Application Classes for more detail.

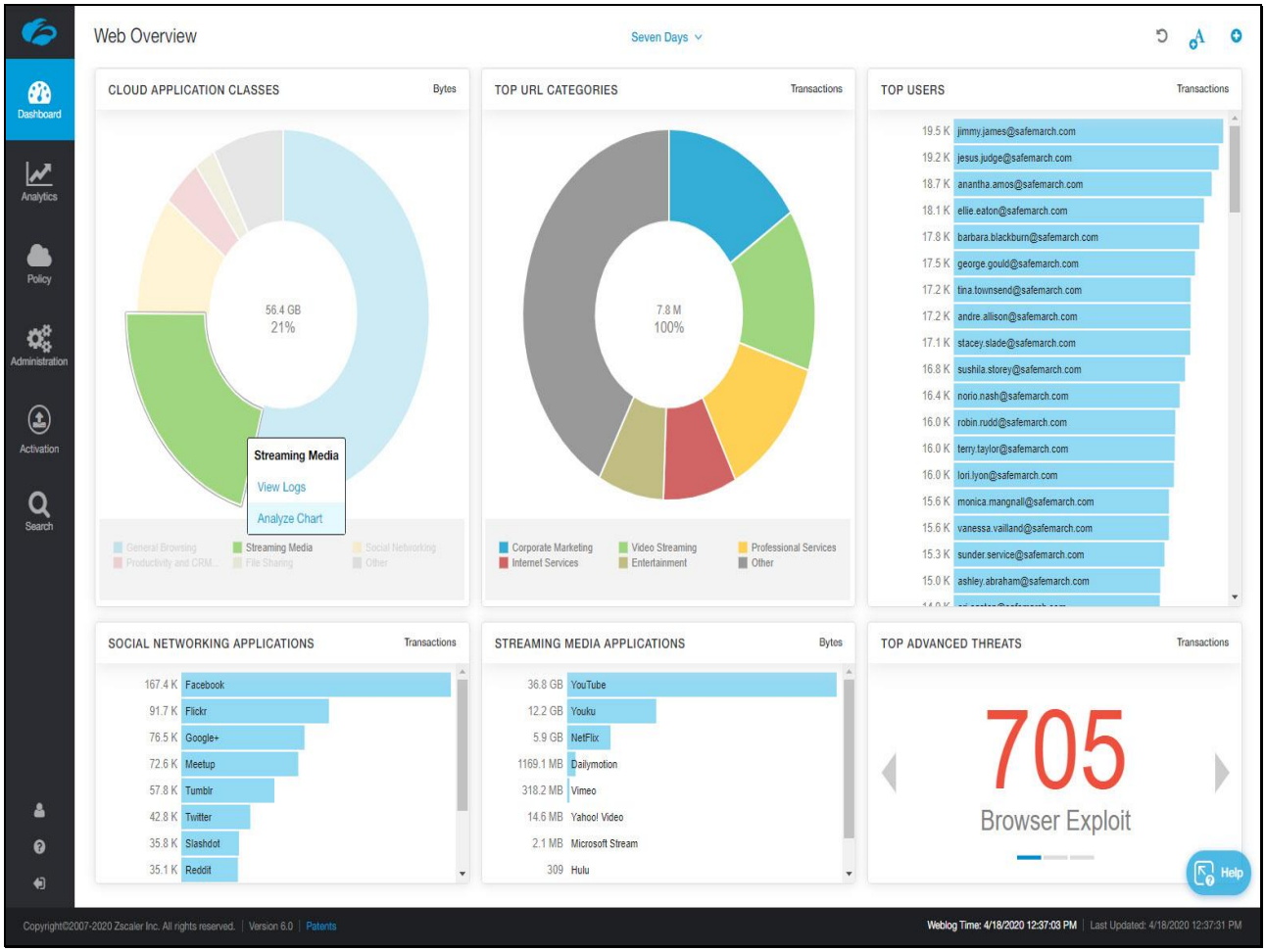
Slide 81 - Slide 81



Slide notes

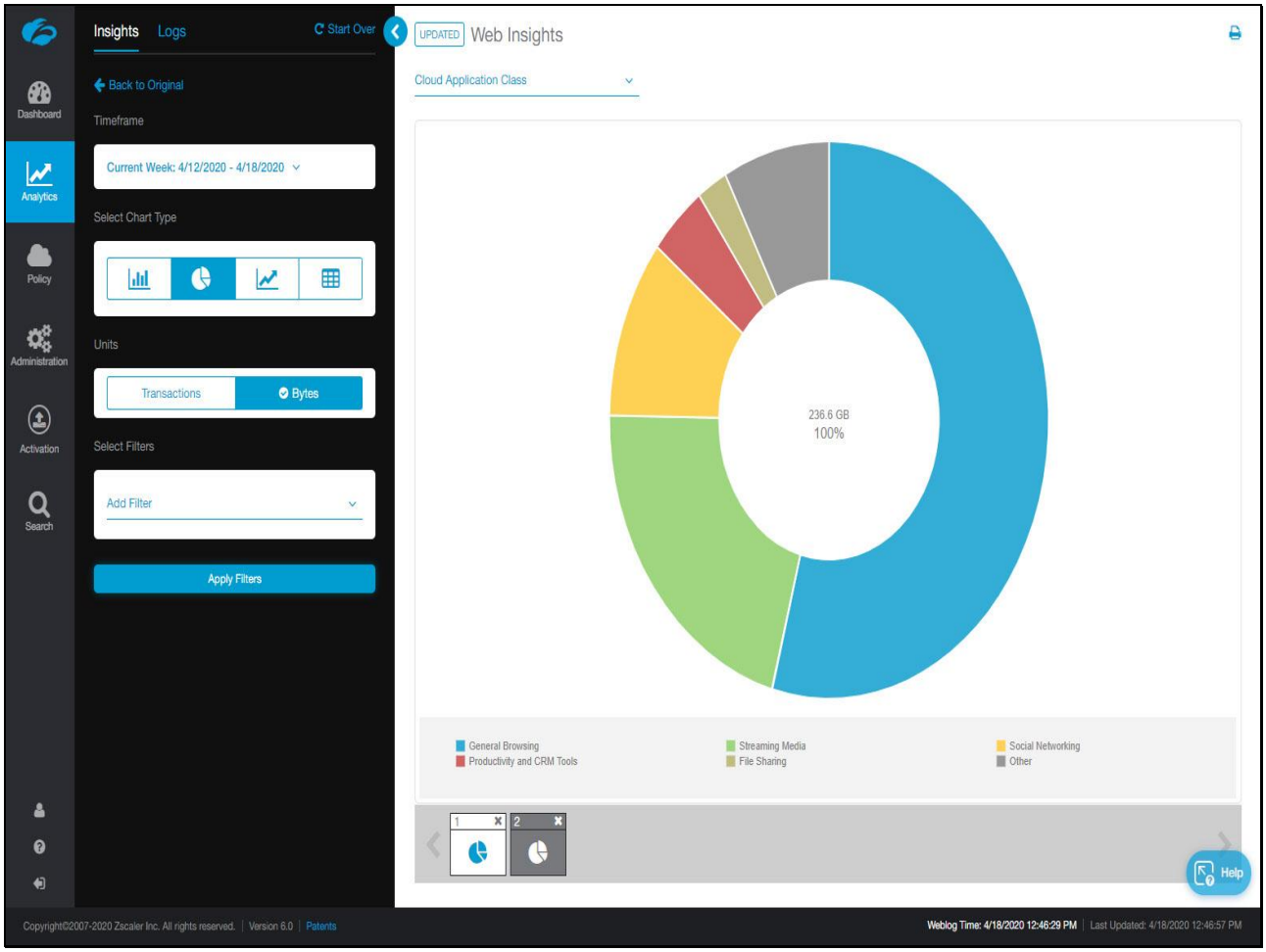
You have the option to view logs to see information such as what users are accessing sites under this application class or analyze the chart for further detail. Click on **Analyze Chart**.

Slide 82 - Slide 82



Slide notes

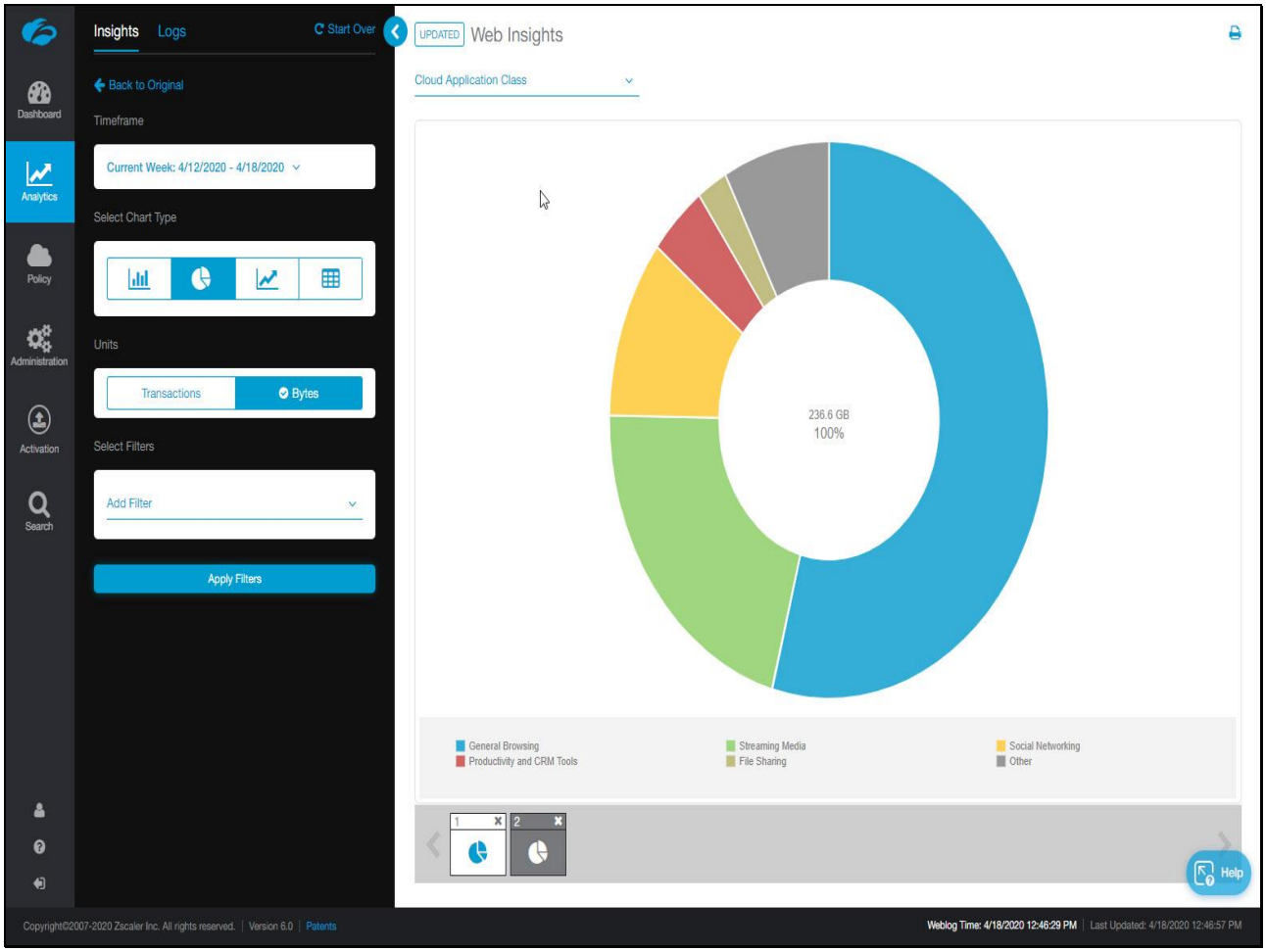
Slide 83 - Slide 83



Slide notes

You are now presented with the same pie chart that you were looking at in the Dashboard but without the distractions of the other widgets. Note that you have also been taken into the Analytics tab at the top of the screen. You can begin your research under the analytics tab, but most find it easier to begin with the high-level view presented in the Dashboard then drill down for more detail. You might start in the Analytics tab if you are looking for a specific issue.

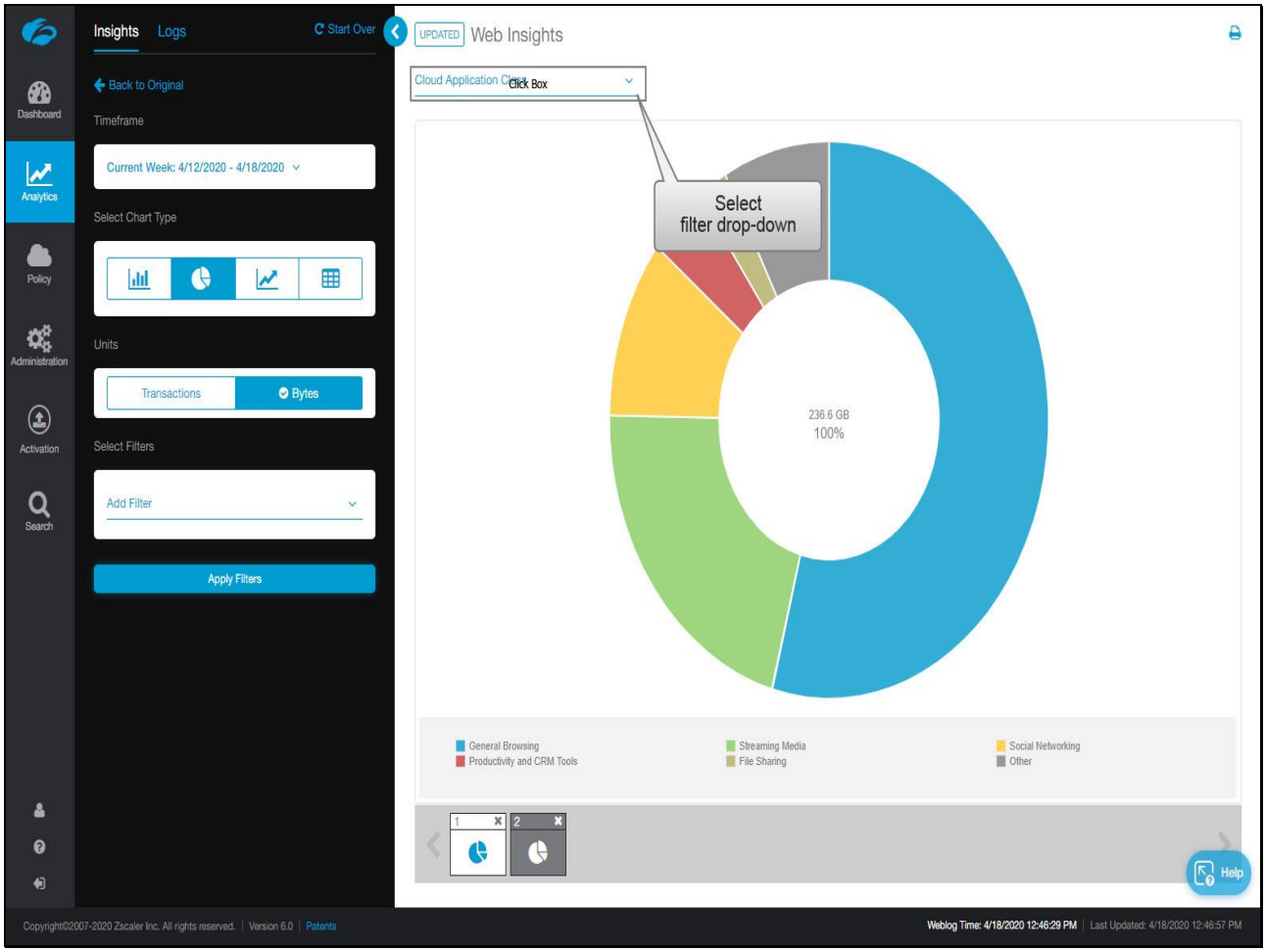
Slide 84 - Slide 84



Slide notes

You can see, again, that Streaming Media is consuming a lot of bandwidth and you, as the Administrator, know that in your organization this has no legitimate business use. But let's investigate further to see what specific application in this category is causing the issue.

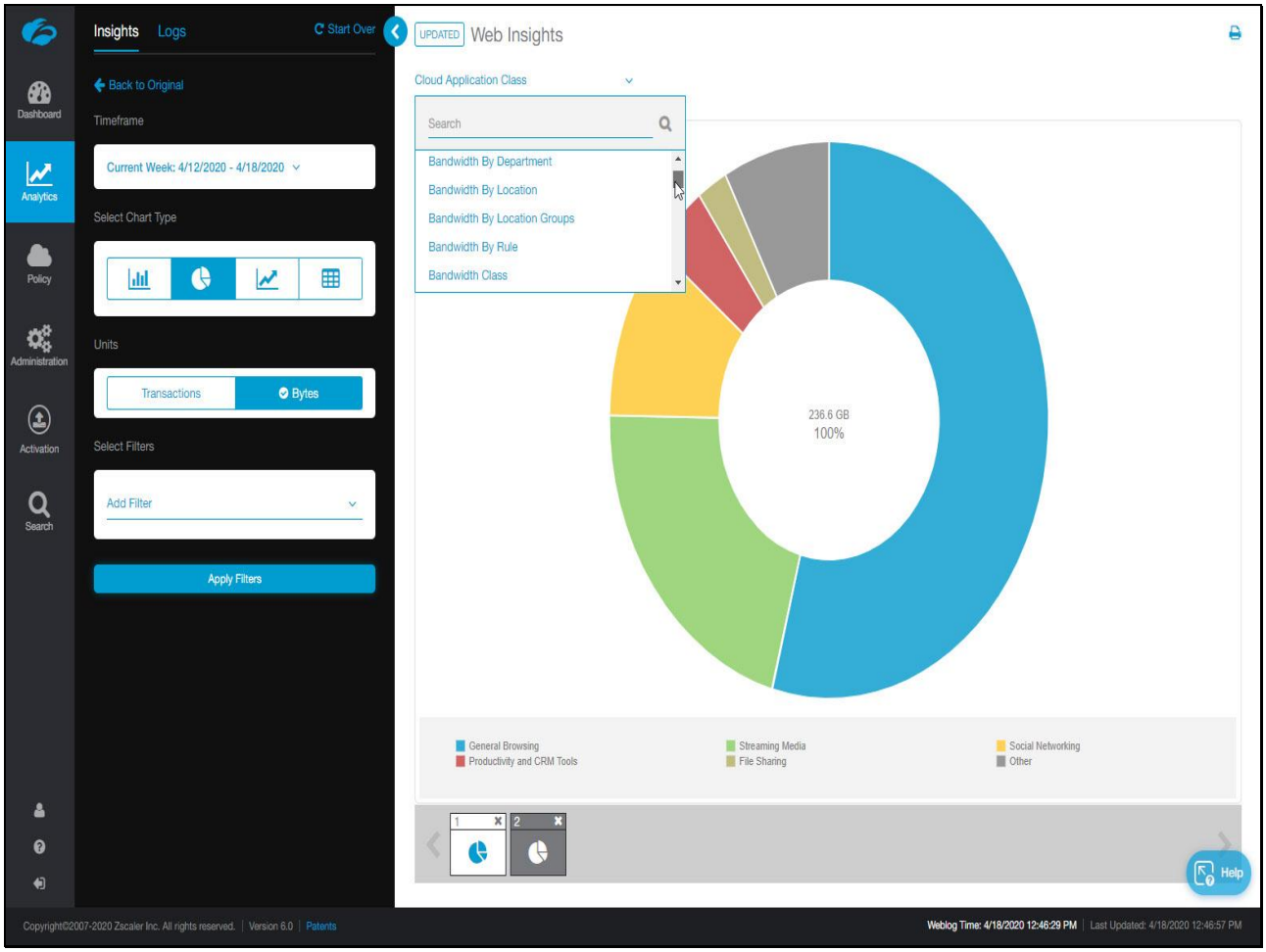
Slide 85 - Slide 85



Slide notes

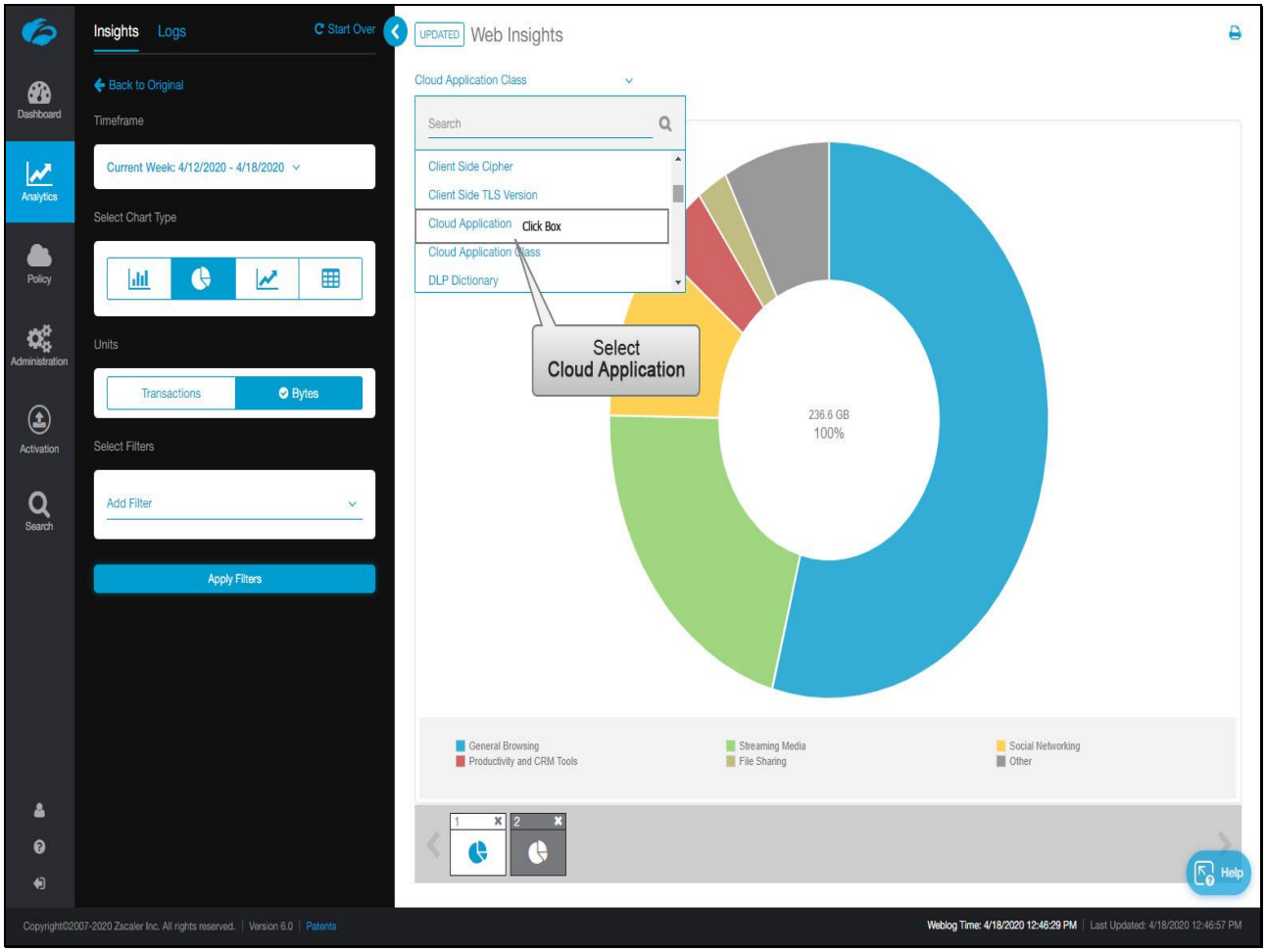
Click on the filter drop down.

Slide 86 - Slide 86



Slide notes

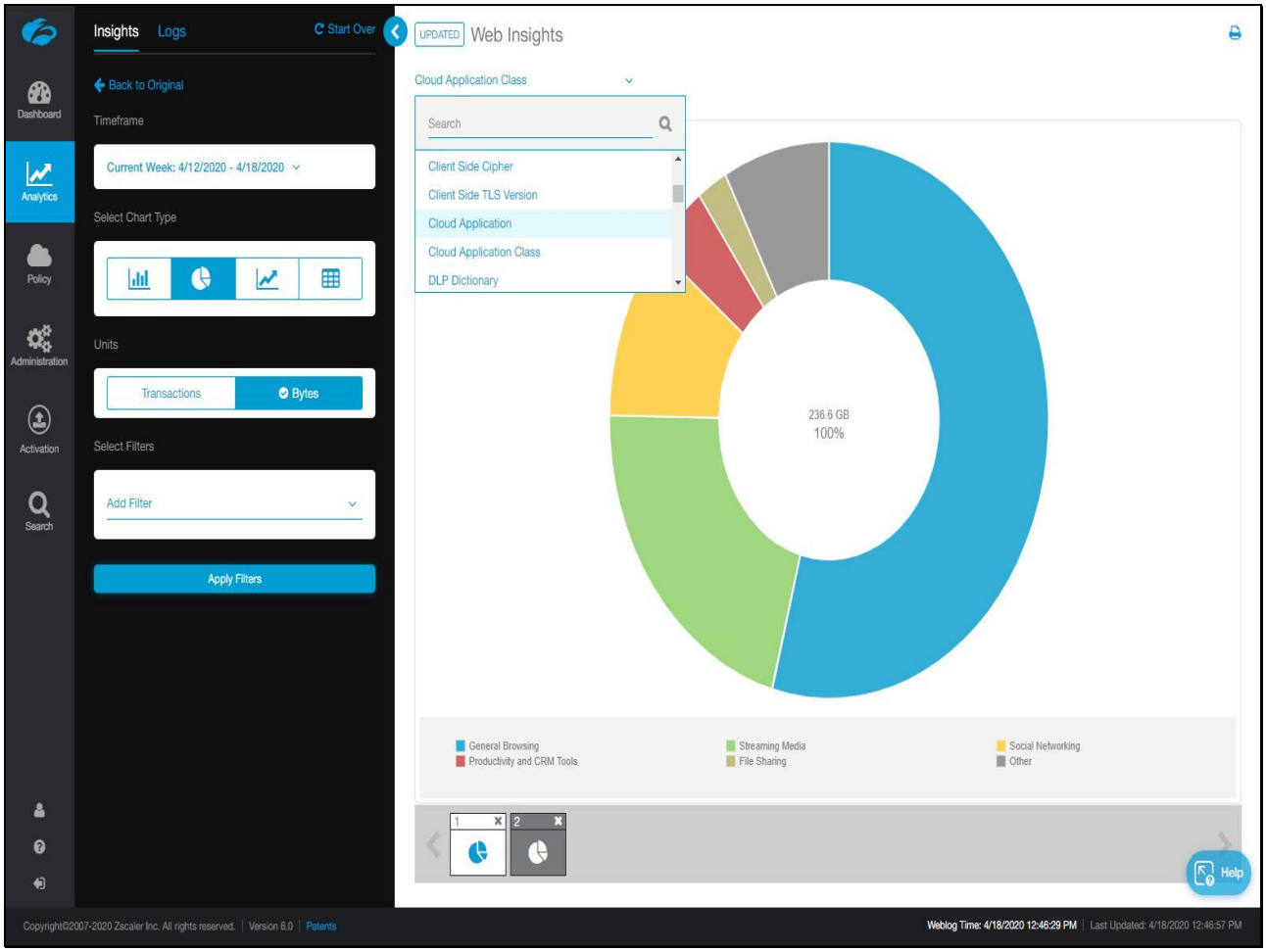
Slide 87 - Slide 87



Slide notes

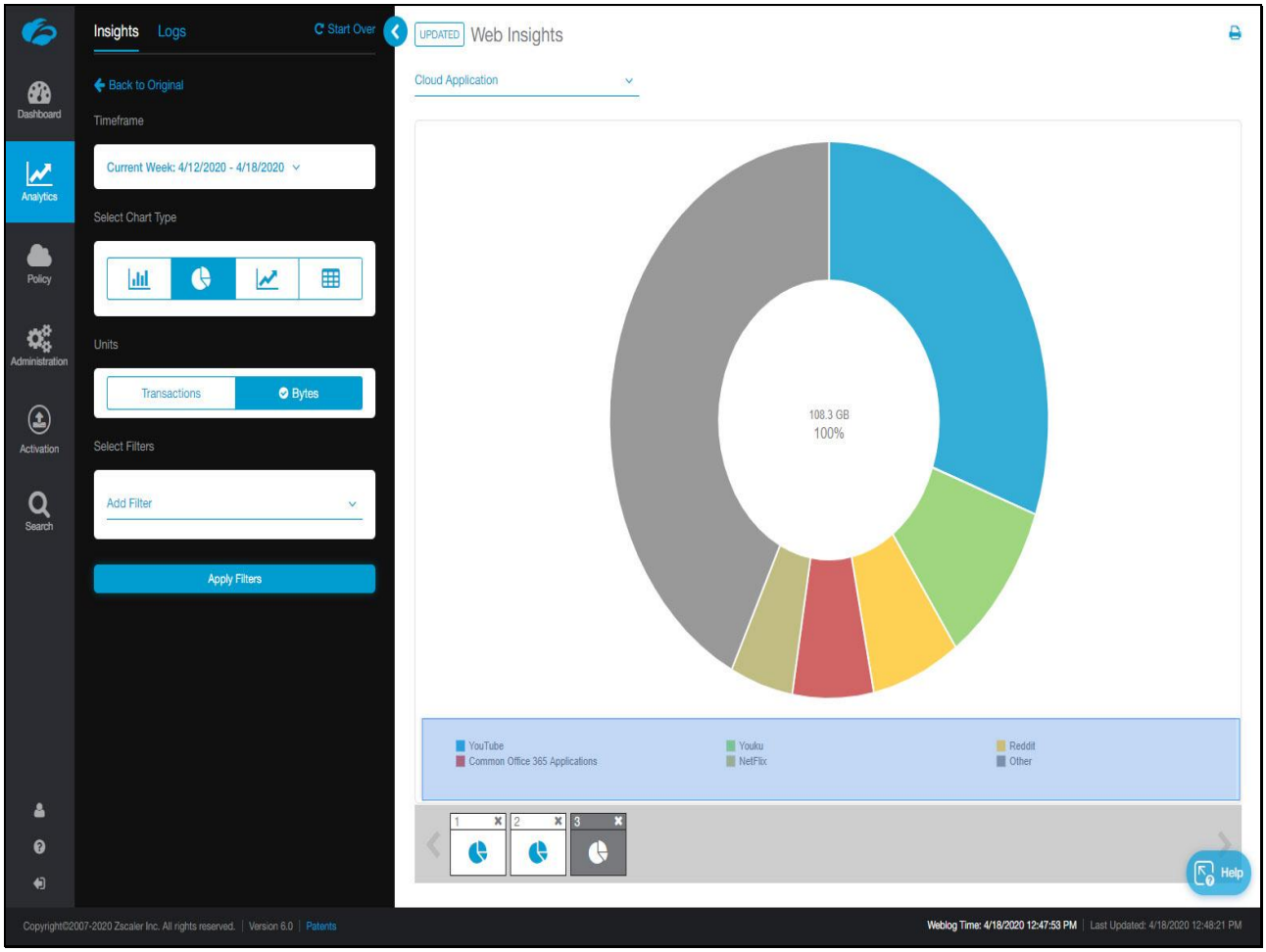
And select "**Cloud Application**".

Slide 88 - Slide 88



Slide notes

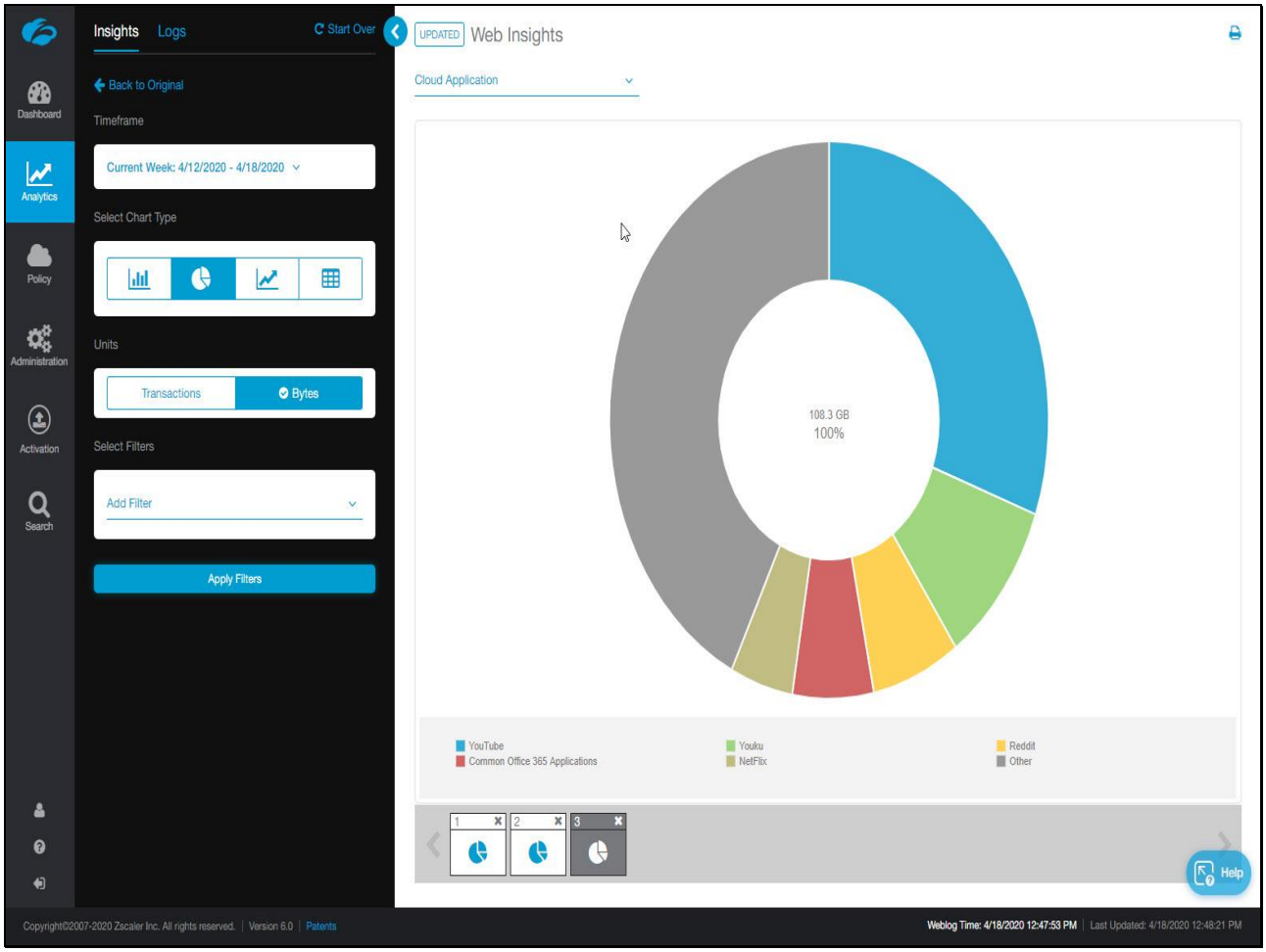
Slide 89 - Slide 89



Slide notes

This changes the chart to show applications by name rather than by category.

Slide 90 - Slide 90

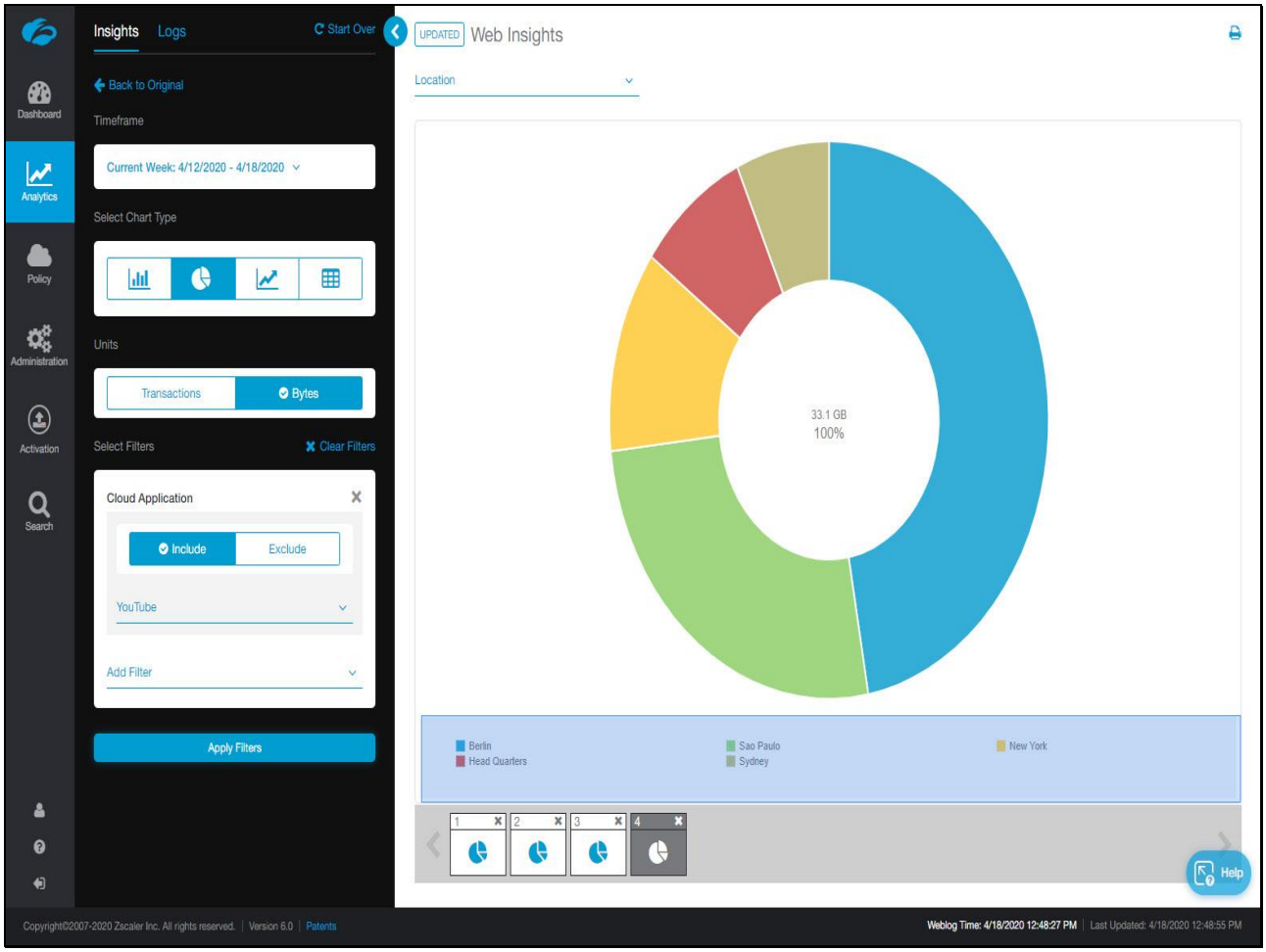


Slide notes

You can see that YouTube is consuming a third of the bandwidth in your network. This is across all of your locations. Let's drill down a little further and see if one location is using YouTube more than others.

You can see that YouTube is consuming a third of the bandwidth in your network. This is across all of your locations.

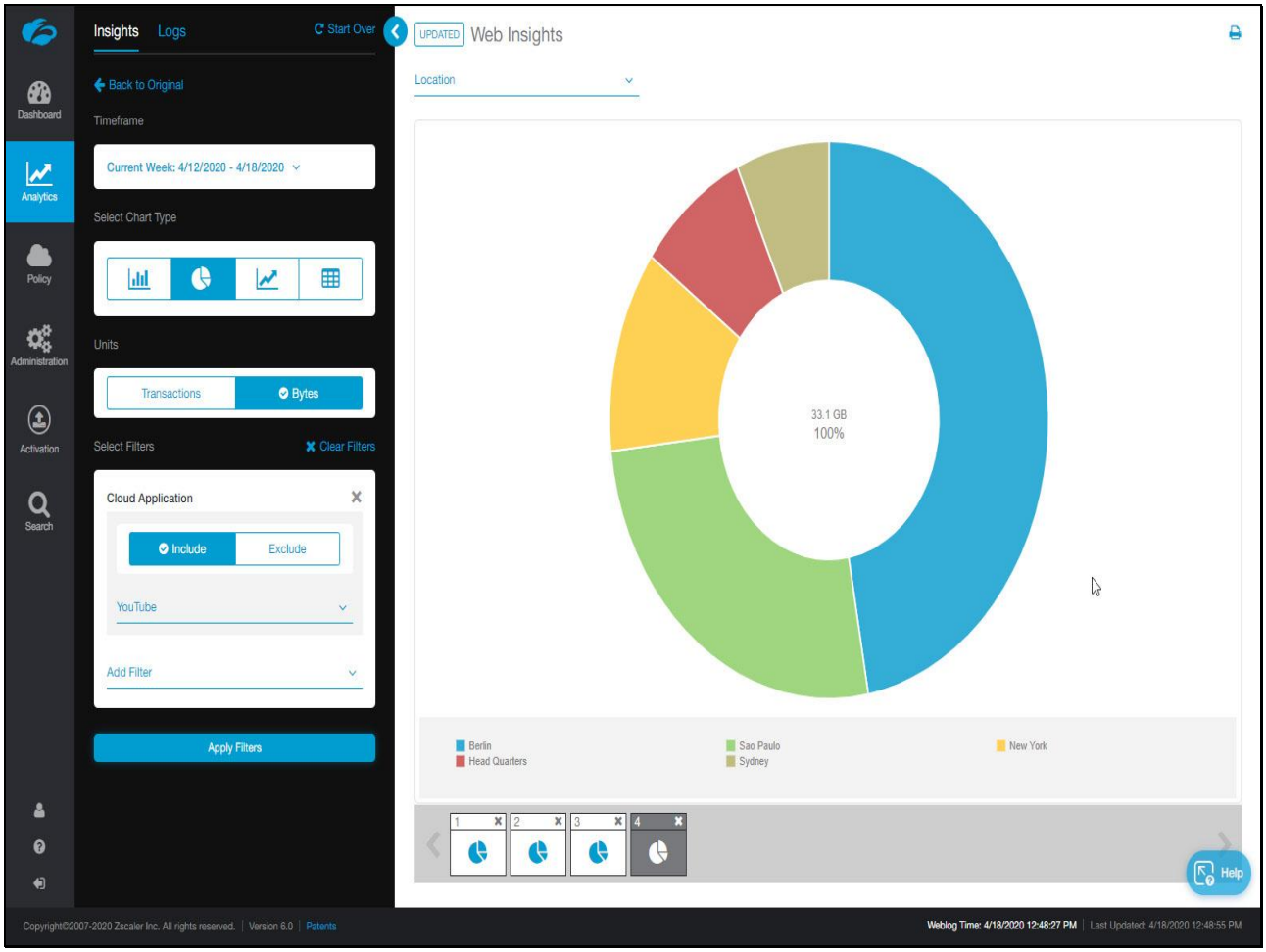
Slide 91 - Slide 91



Slide notes

The chart has now updated to show the locations on your network.

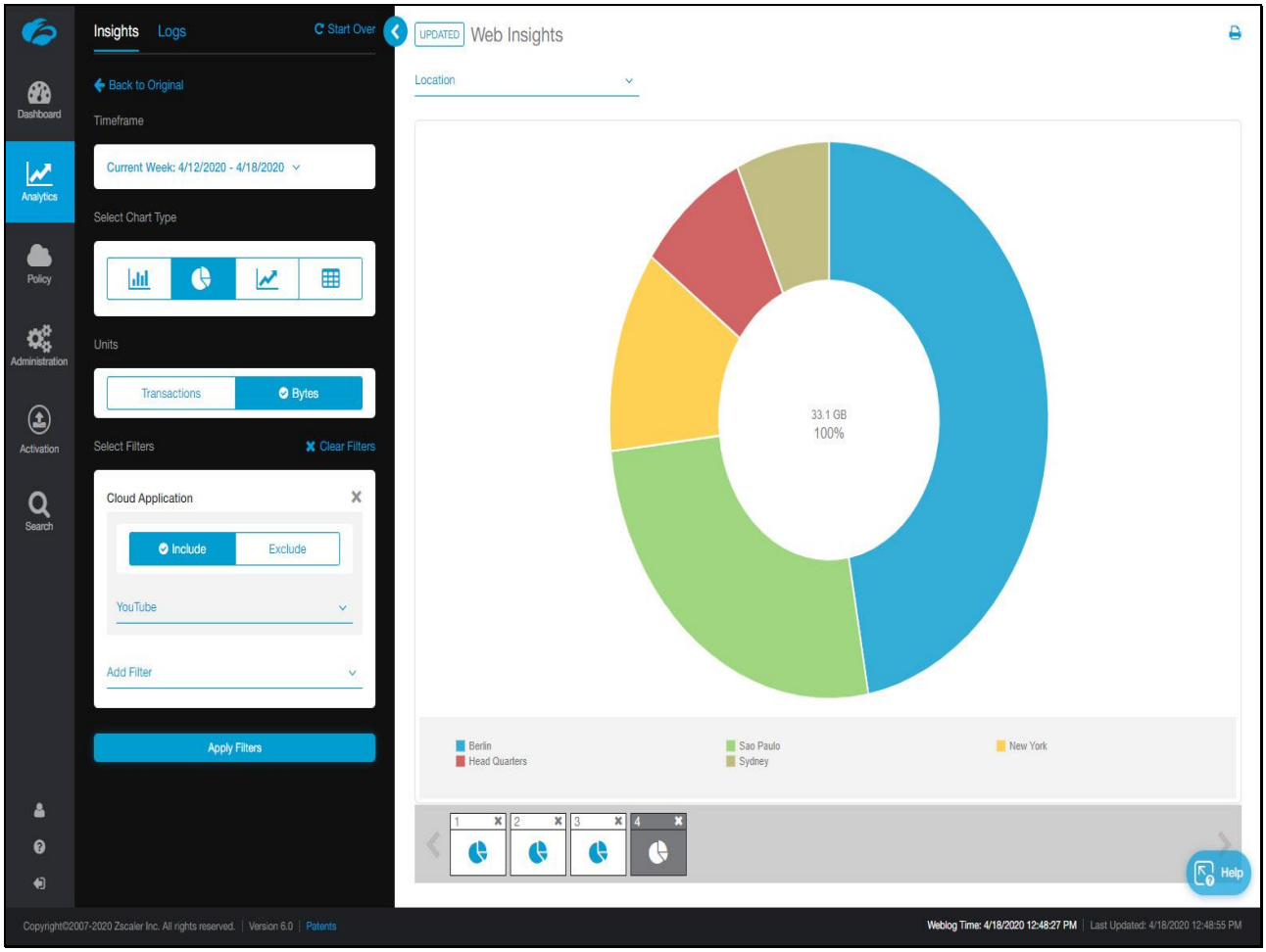
Slide 92 - Slide 92



Slide notes

As you move your mouse across the chart you can see that Berlin and San Paulo are spending the most time on YouTube.

Slide 93 - Slide 93

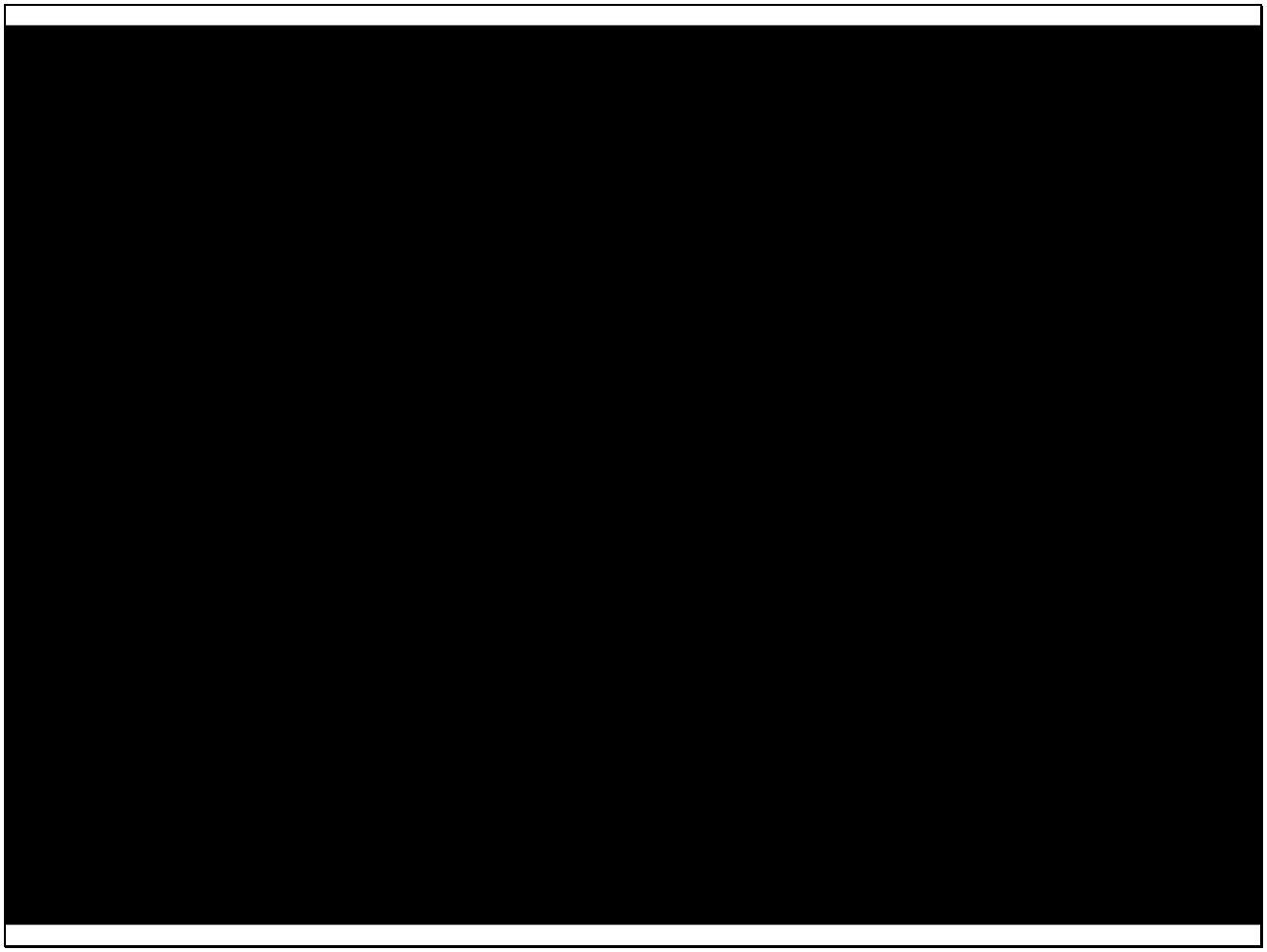


Slide notes

At this point you need to decide on how to tackle this issue. As Streaming Media, particularly YouTube, has no business use case for your organization you need to decide to block it companywide, block it for the sites that are the worst offenders, or, allow it but with restrictions such as allowing it after working hours.

These are all options you can configure under Policy configuration which is covered in a separate module. For now, let's assume that blocking YouTube companywide is the right solution. I will configure this policy off screen, and we will look at the results in just a moment.

Slide 94 - Slide 94



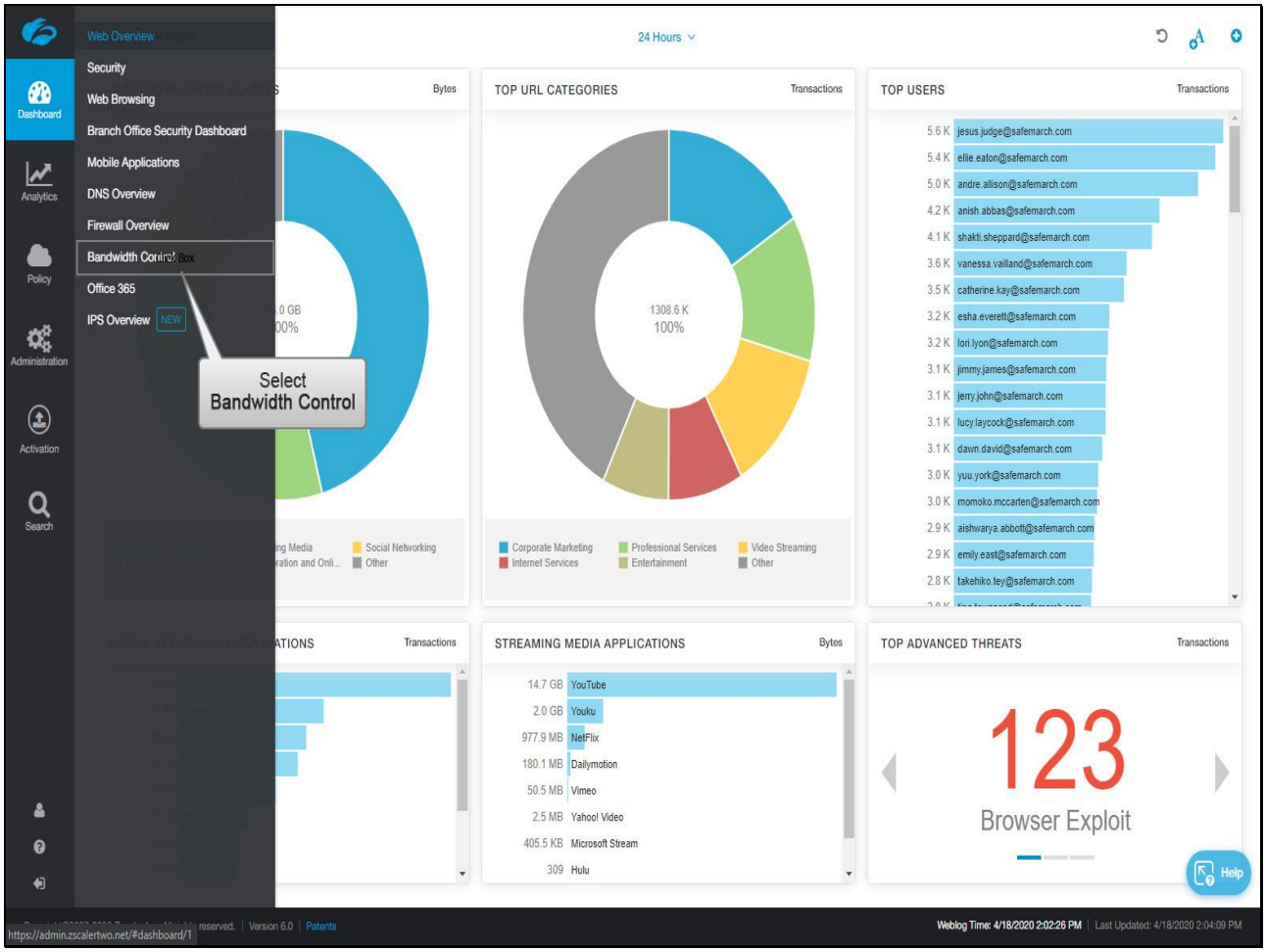
Slide notes

Slide 95 - Slide 95

Slide notes

We are back on the Dashboard and I have configured a Policy to block YouTube. Rather than using the Web Overview dashboard that we used earlier let's look at the Bandwidth Control dashboard to see our results. Click on the **Dashboard tab**.

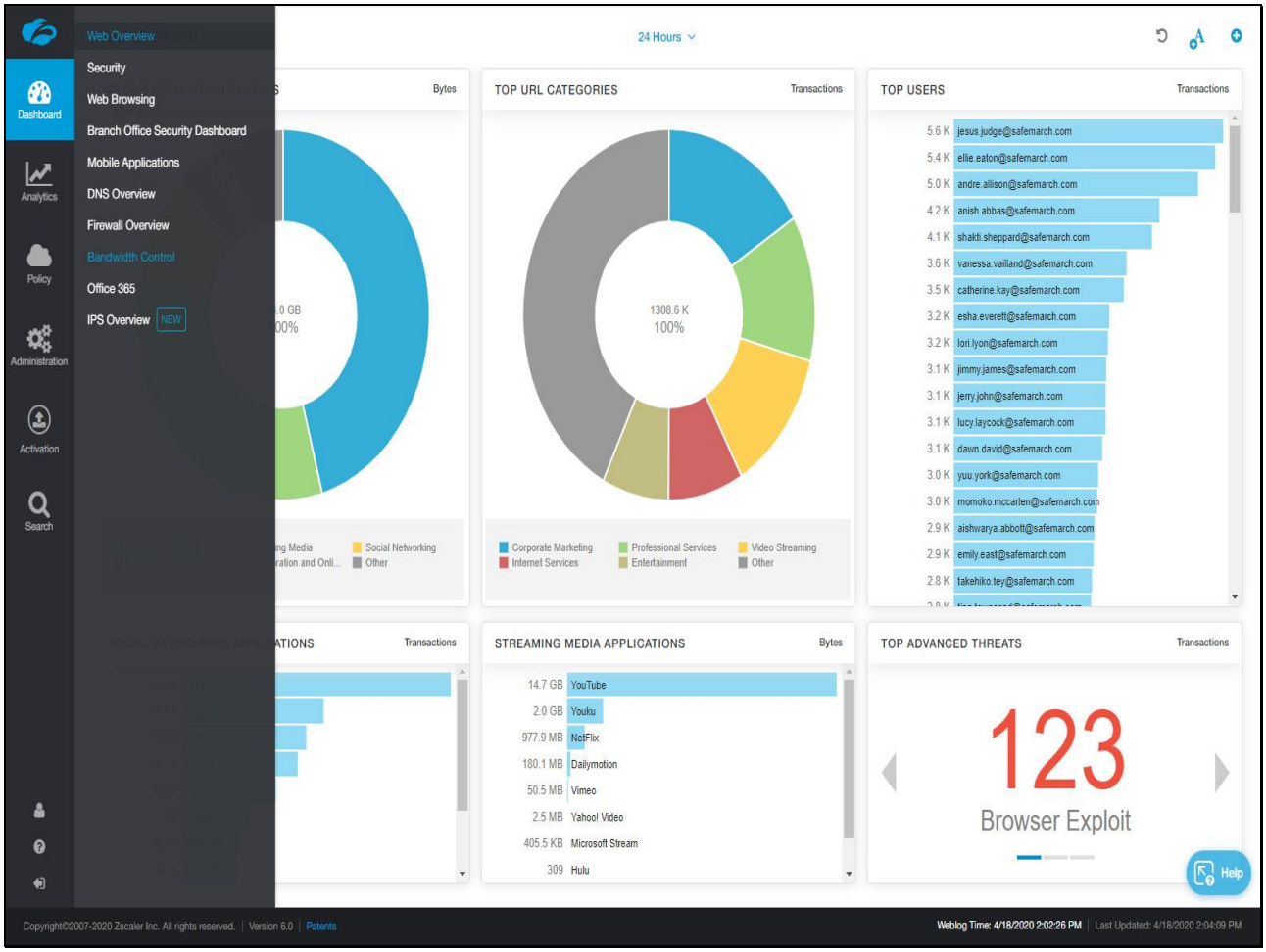
Slide 96 - Slide 96



Slide notes

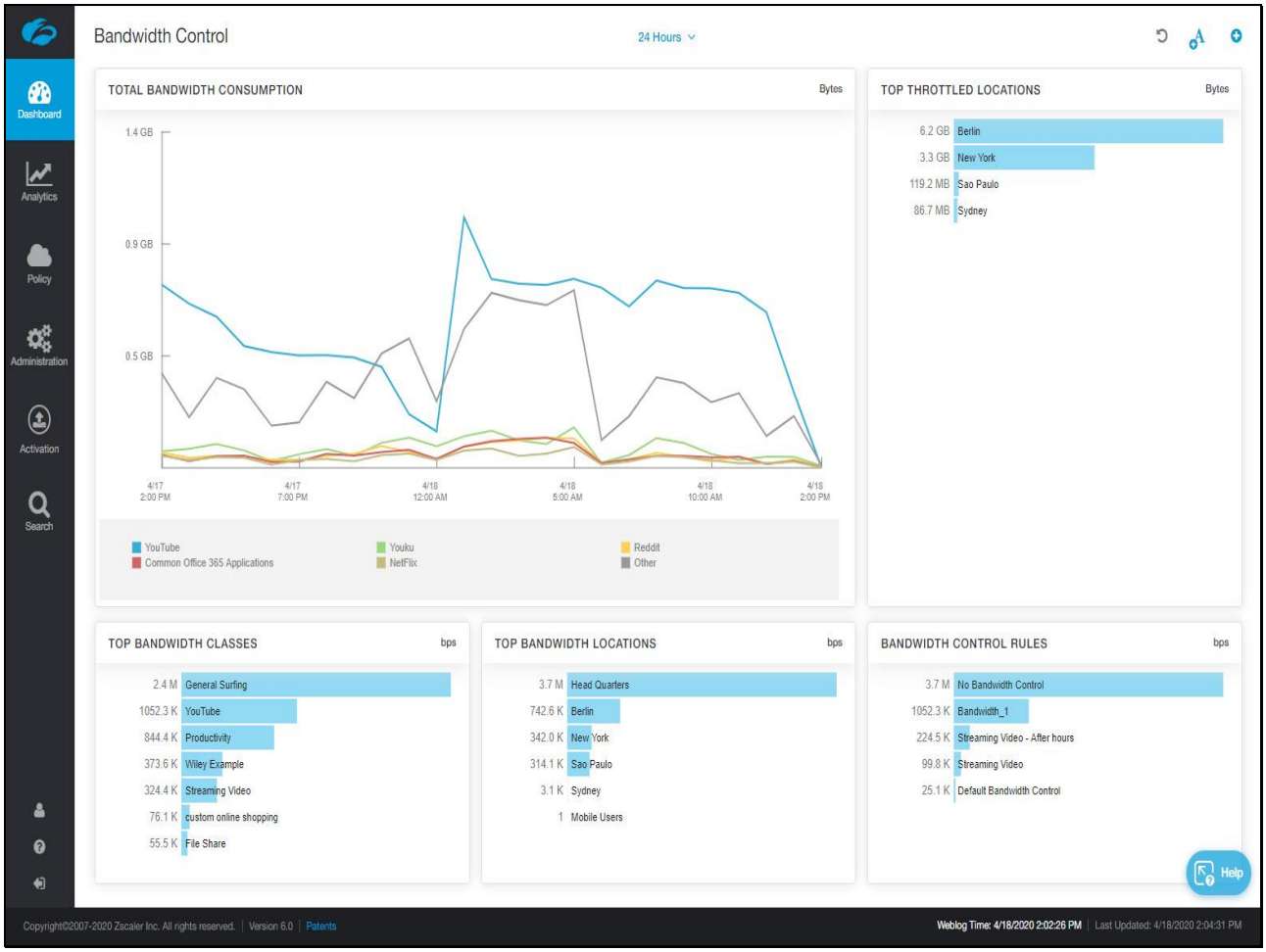
And select **Bandwidth Control**.

Slide 97 - Slide 97



Slide notes

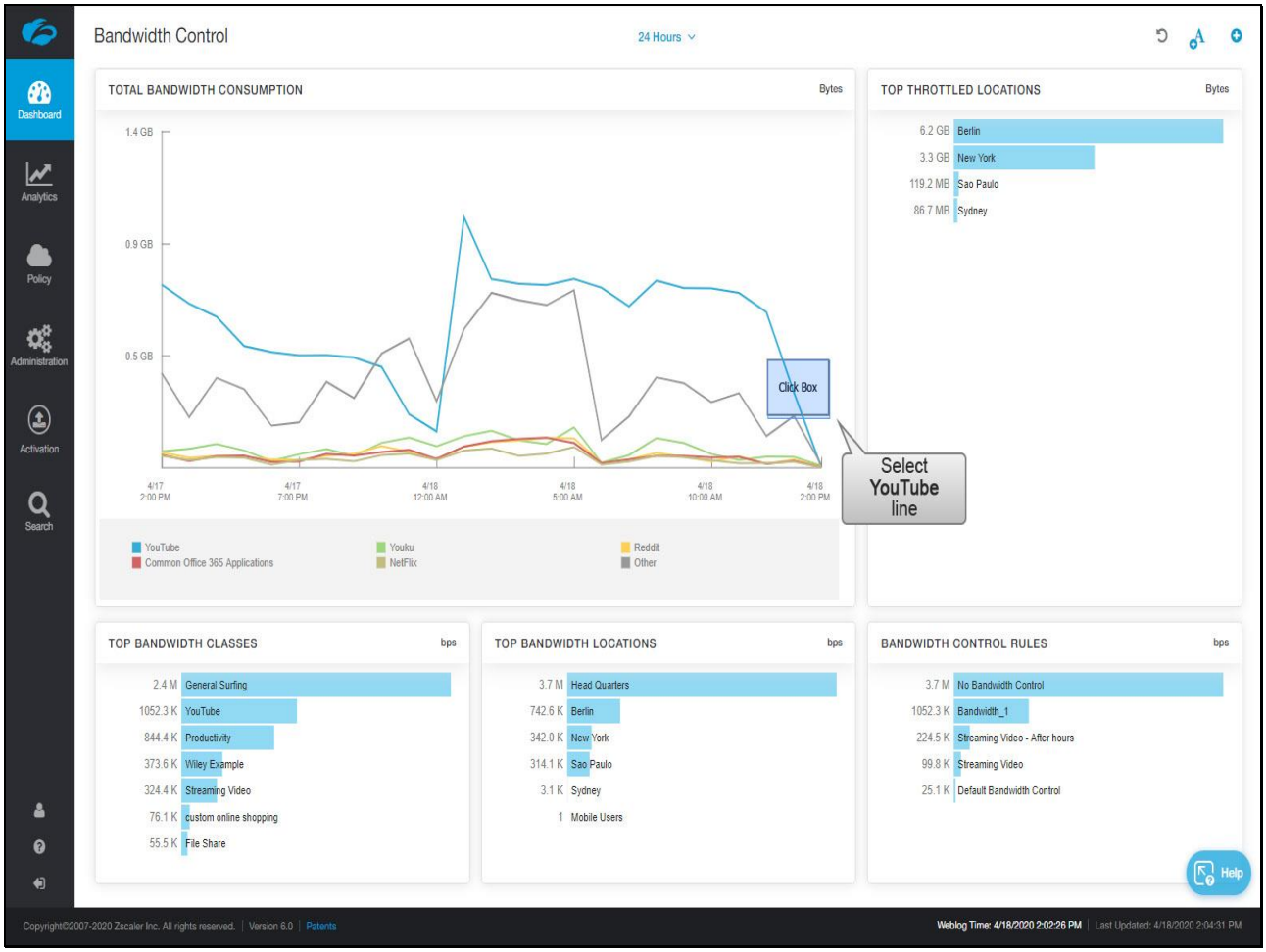
Slide 98 - Slide 98



Slide notes

Looking at the line graph in the upper left corner you see a breakdown of your bandwidth consumption by application.

Slide 99 - Slide 99

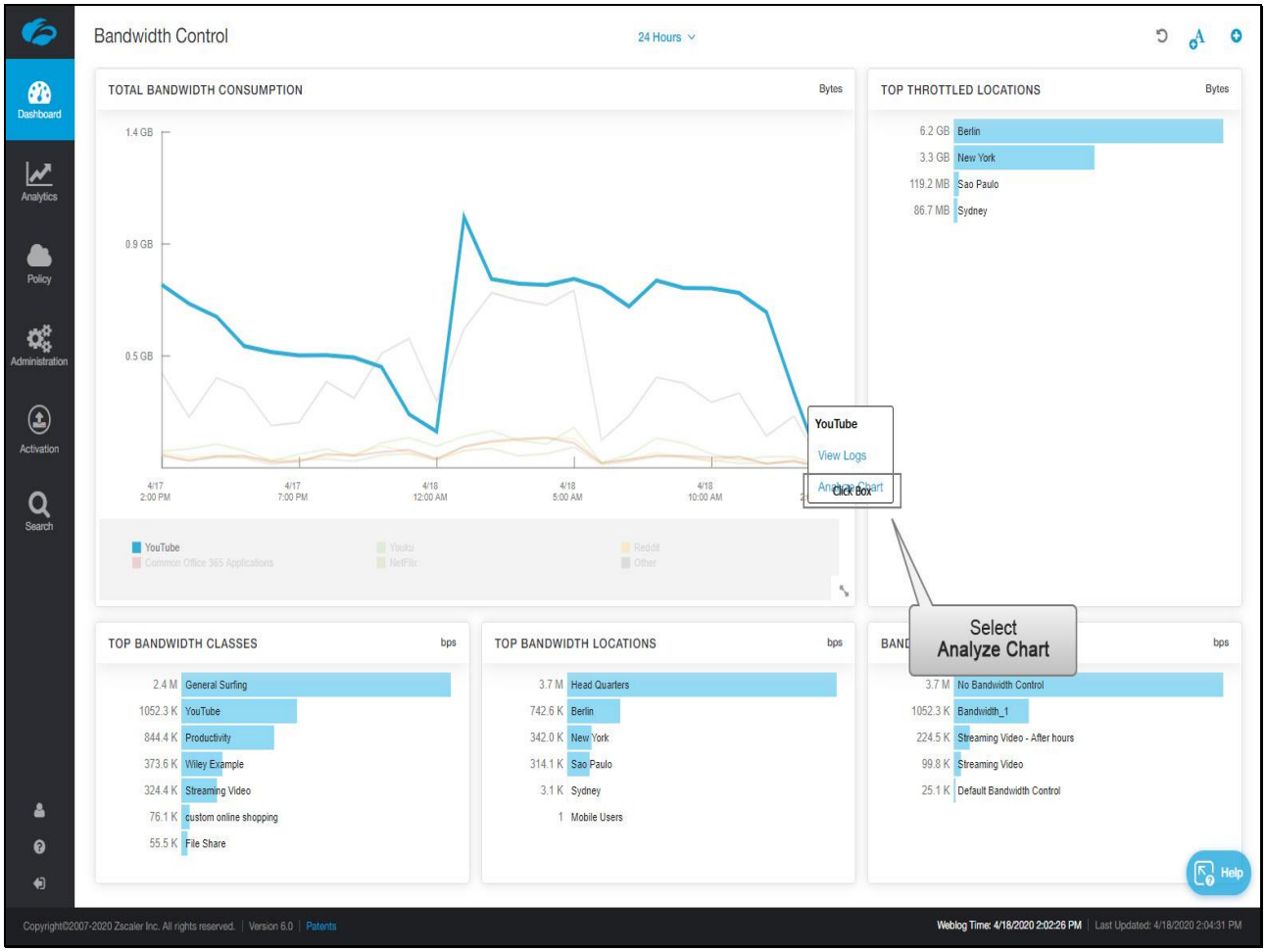


Slide notes

Looking at the line graph in the upper left corner you see a breakdown of your bandwidth consumption by application.

You can see a sharp drop-off in YouTube traffic as a result of the policy put in place to block YouTube. Click on YouTube for more detail.

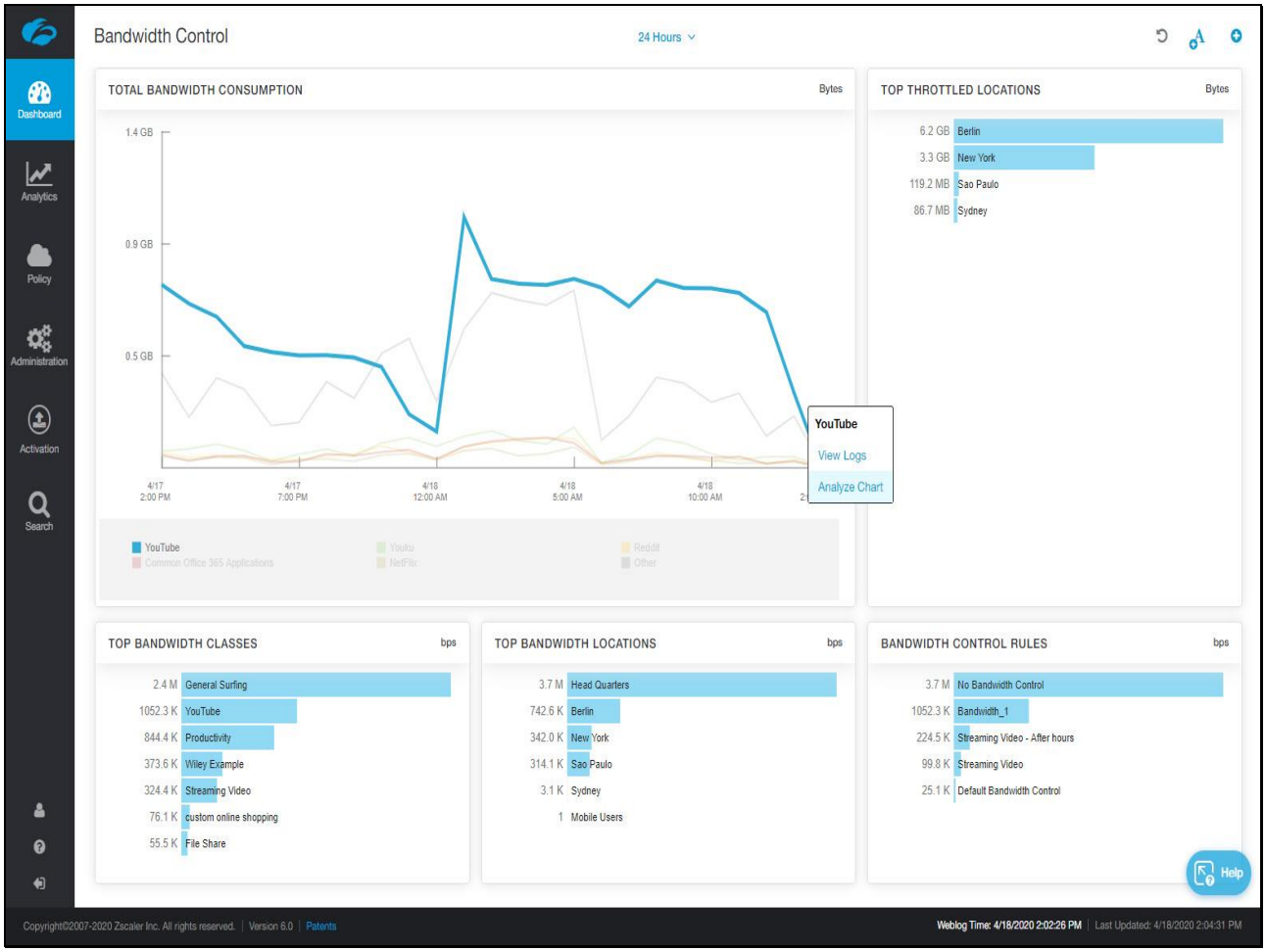
Slide 100 - Slide 100



Slide notes

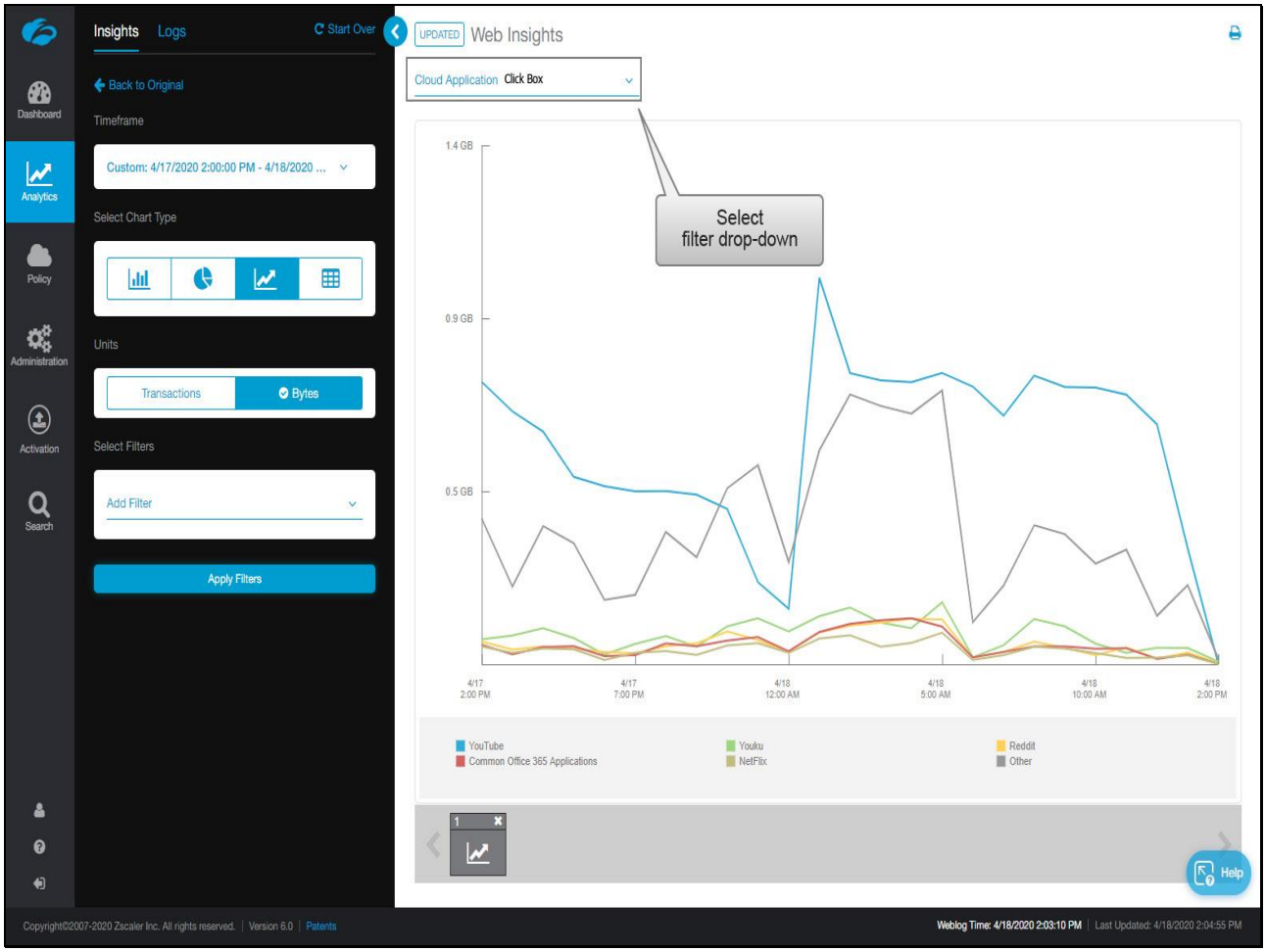
Select **Analyze Chart**.

Slide 101 - Slide 101



Slide notes

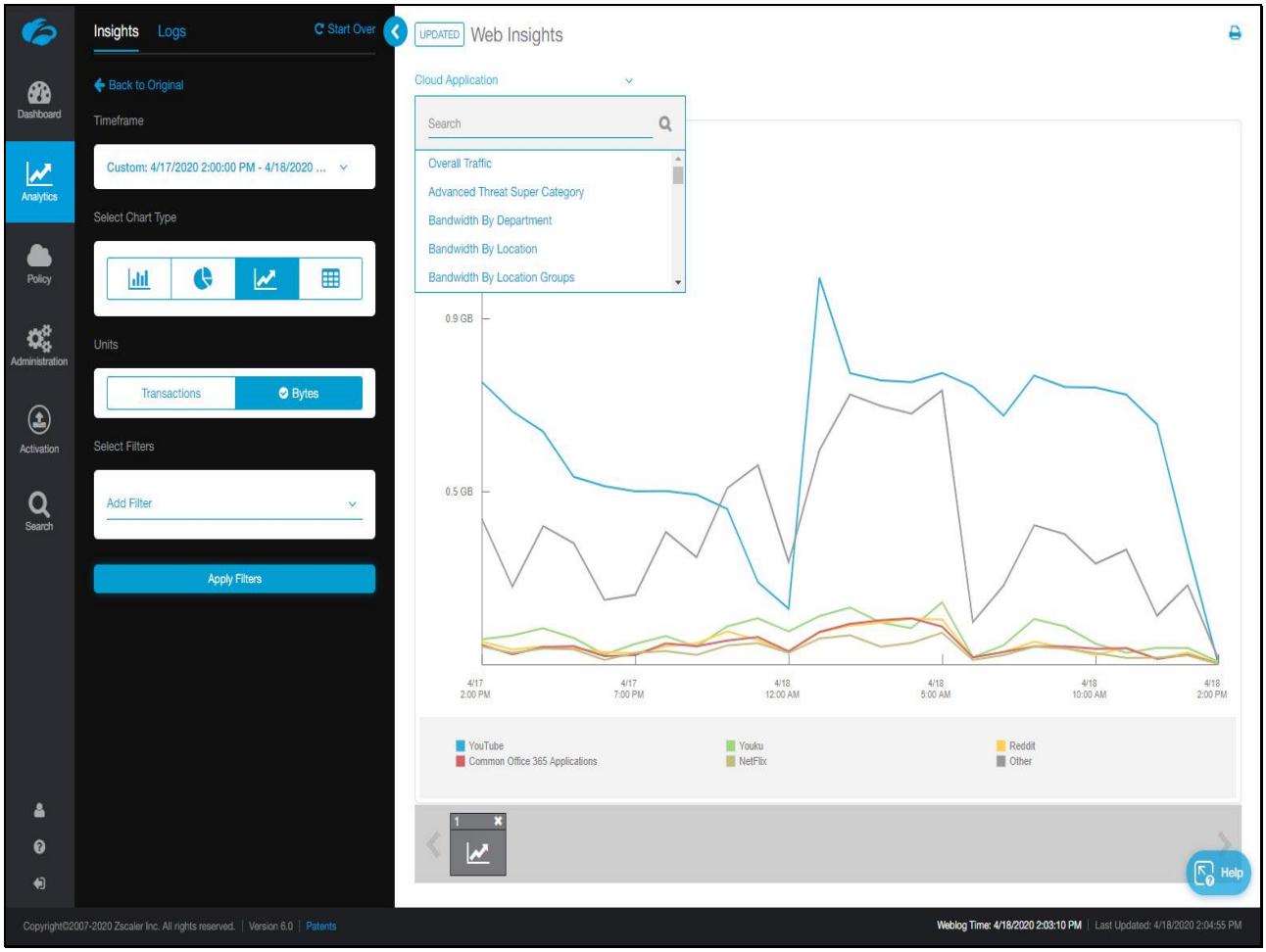
Slide 102 - Slide 102



Slide notes

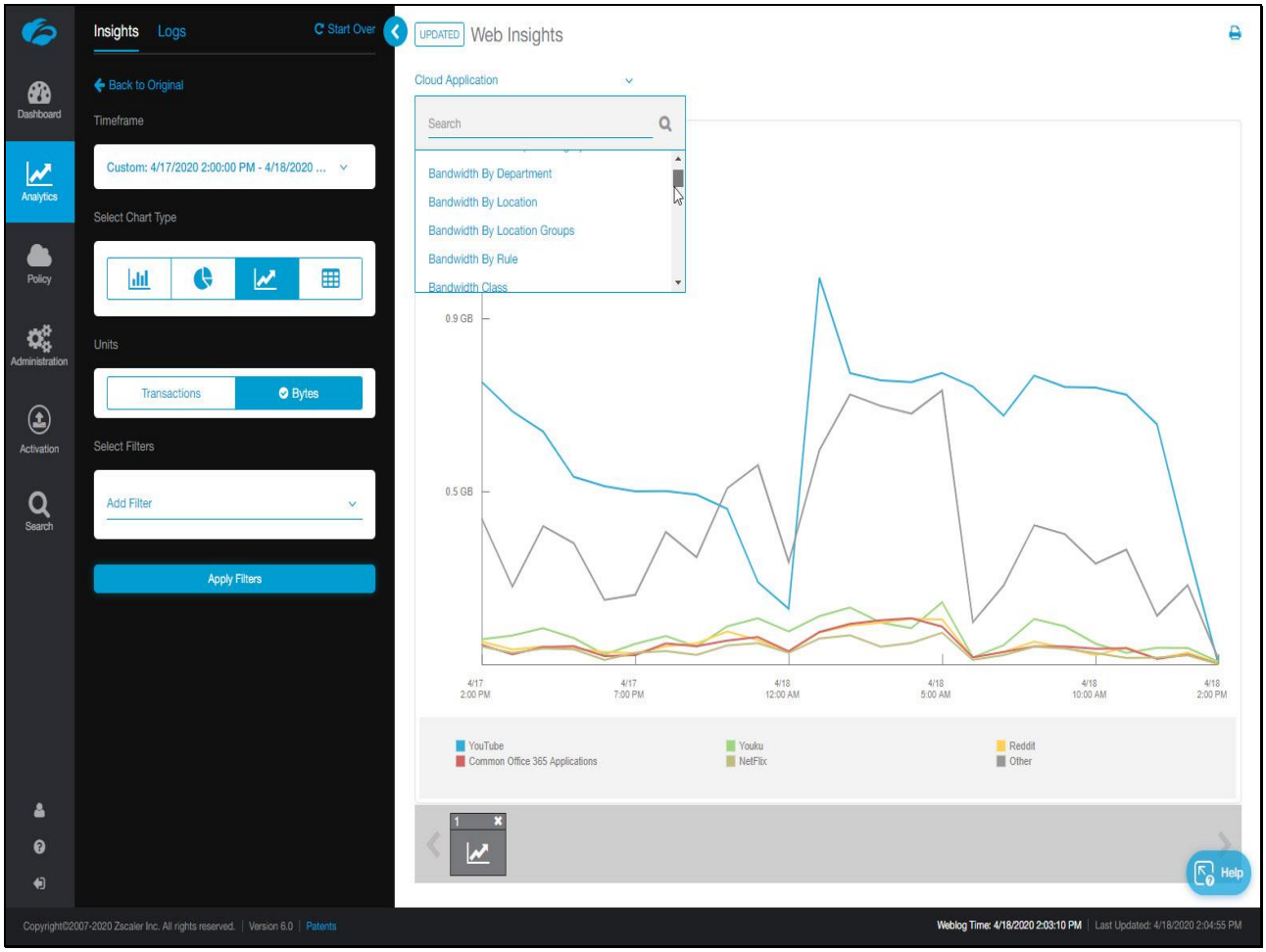
Select the filter drop-down.

Slide 103 - Slide 103



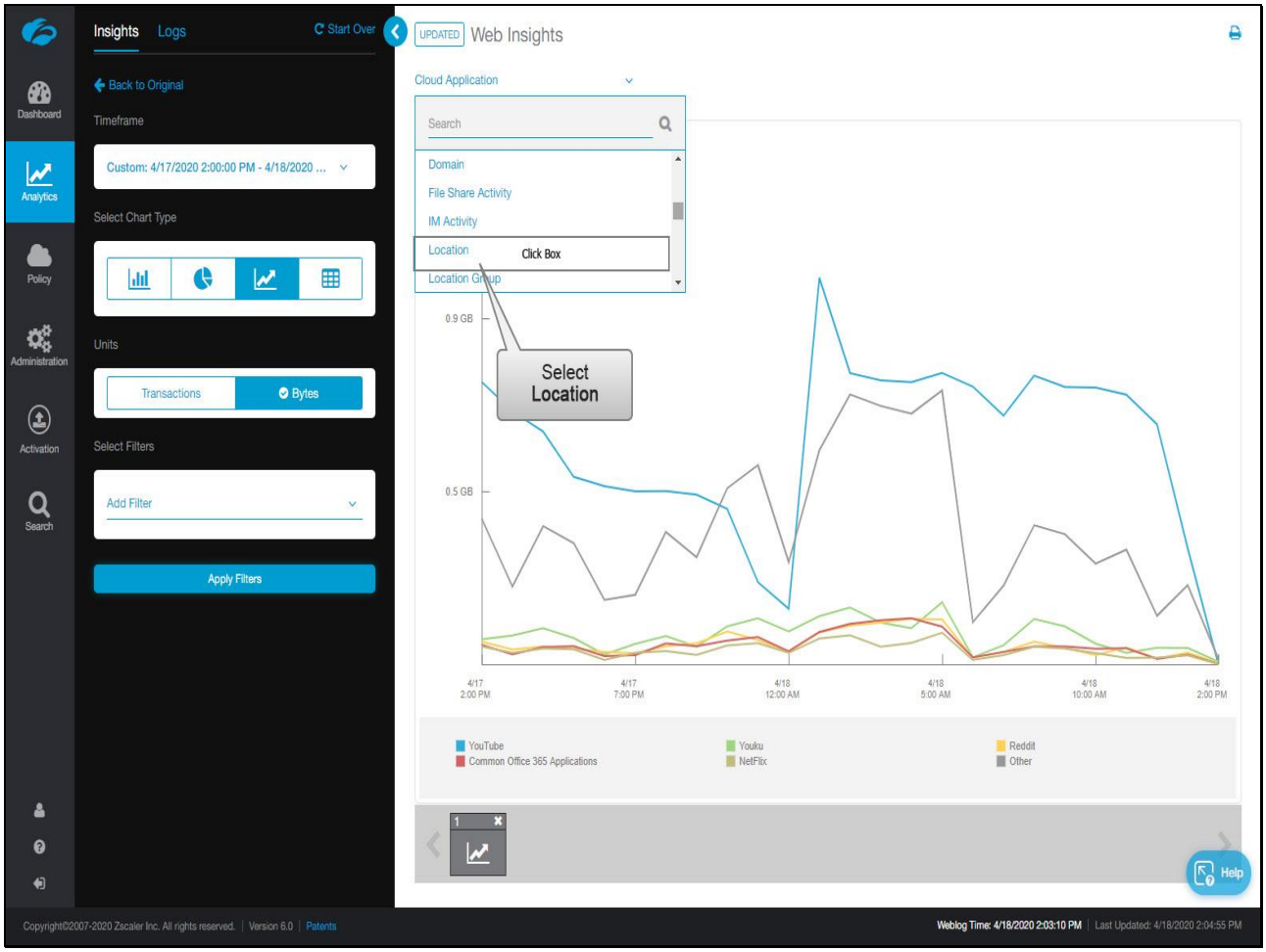
Slide notes

Slide 104 - Slide 104



Slide notes

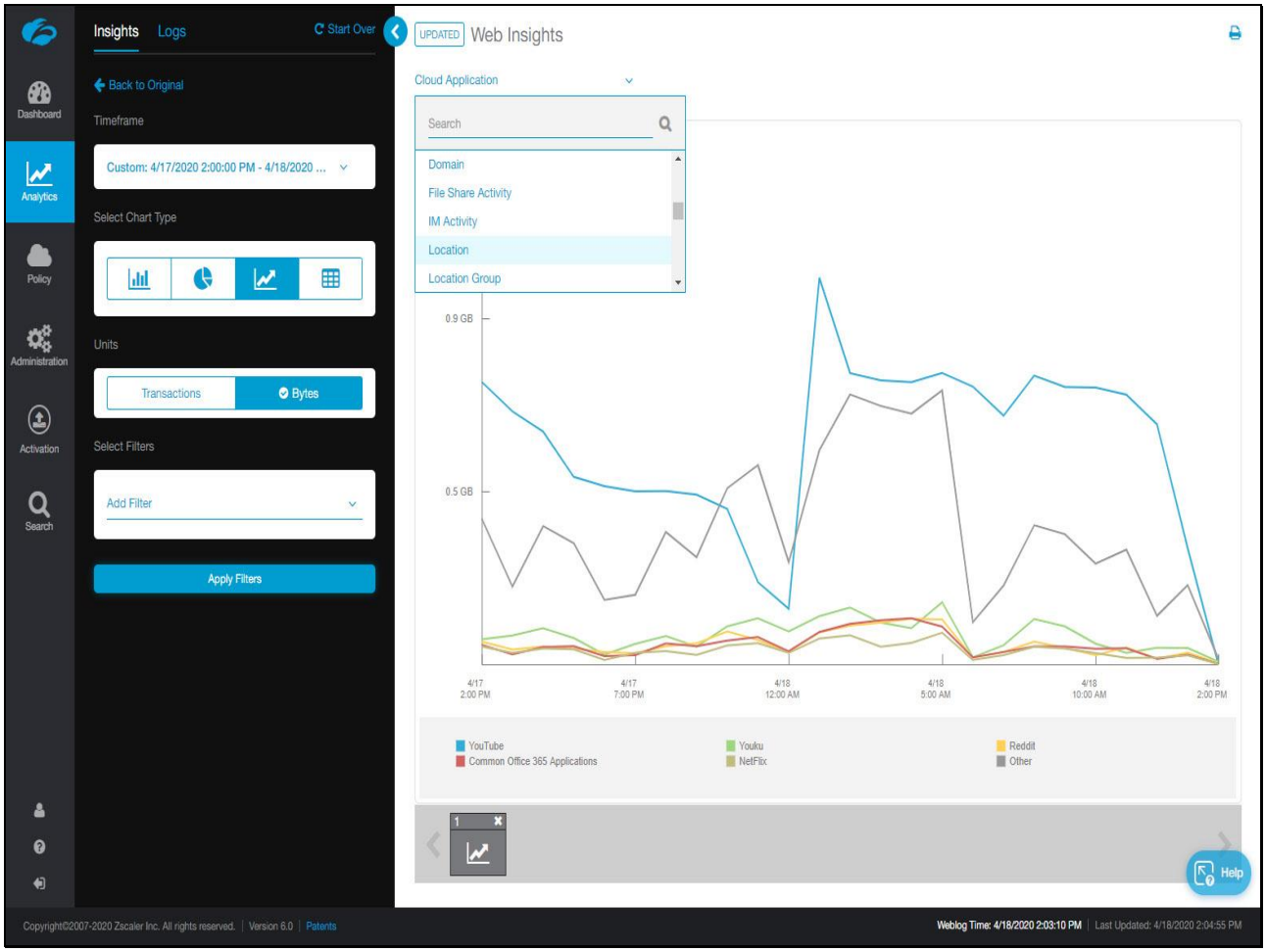
Slide 105 - Slide 105



Slide notes

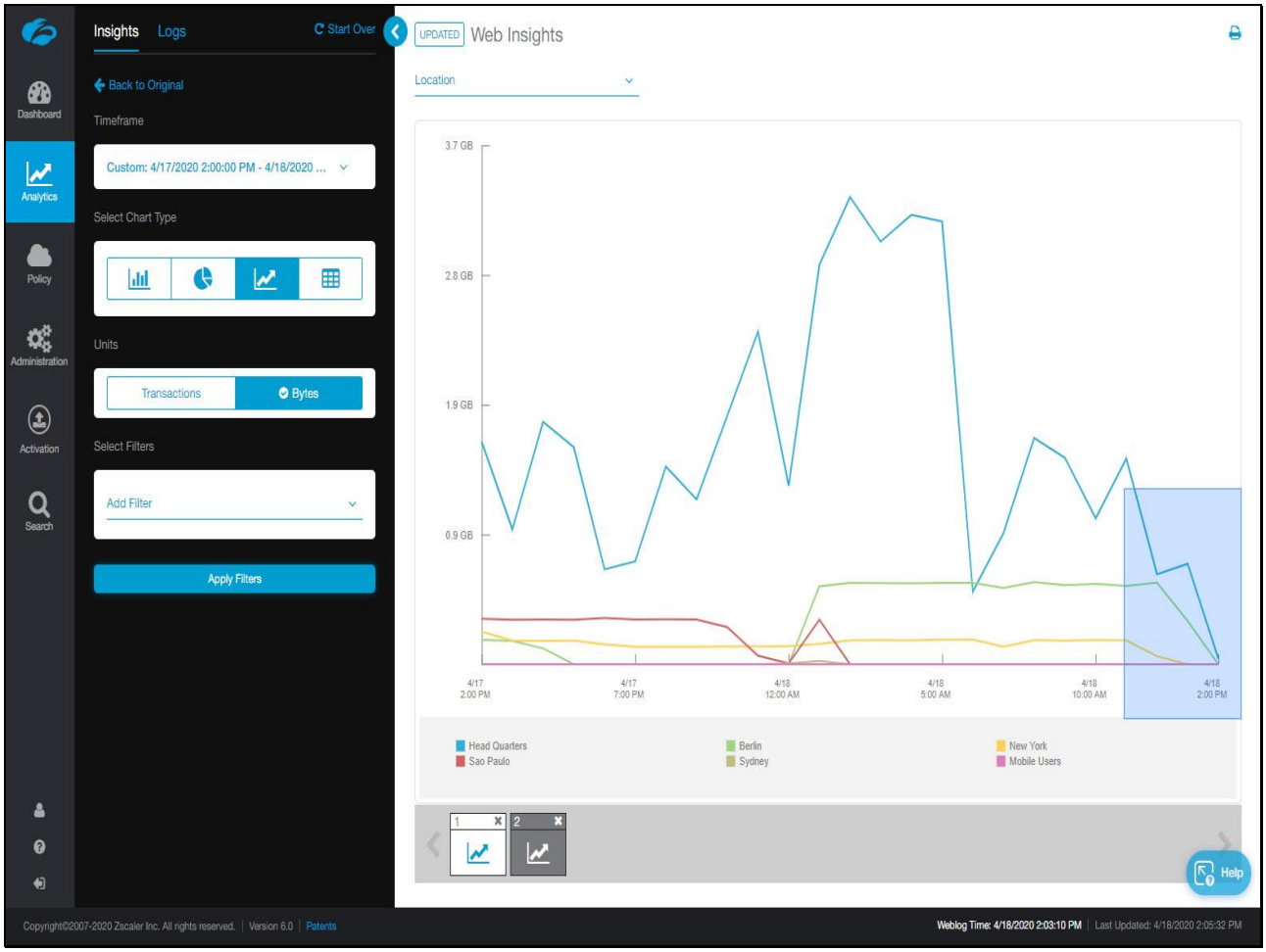
And select **Location**.

Slide 106 - Slide 106



Slide notes

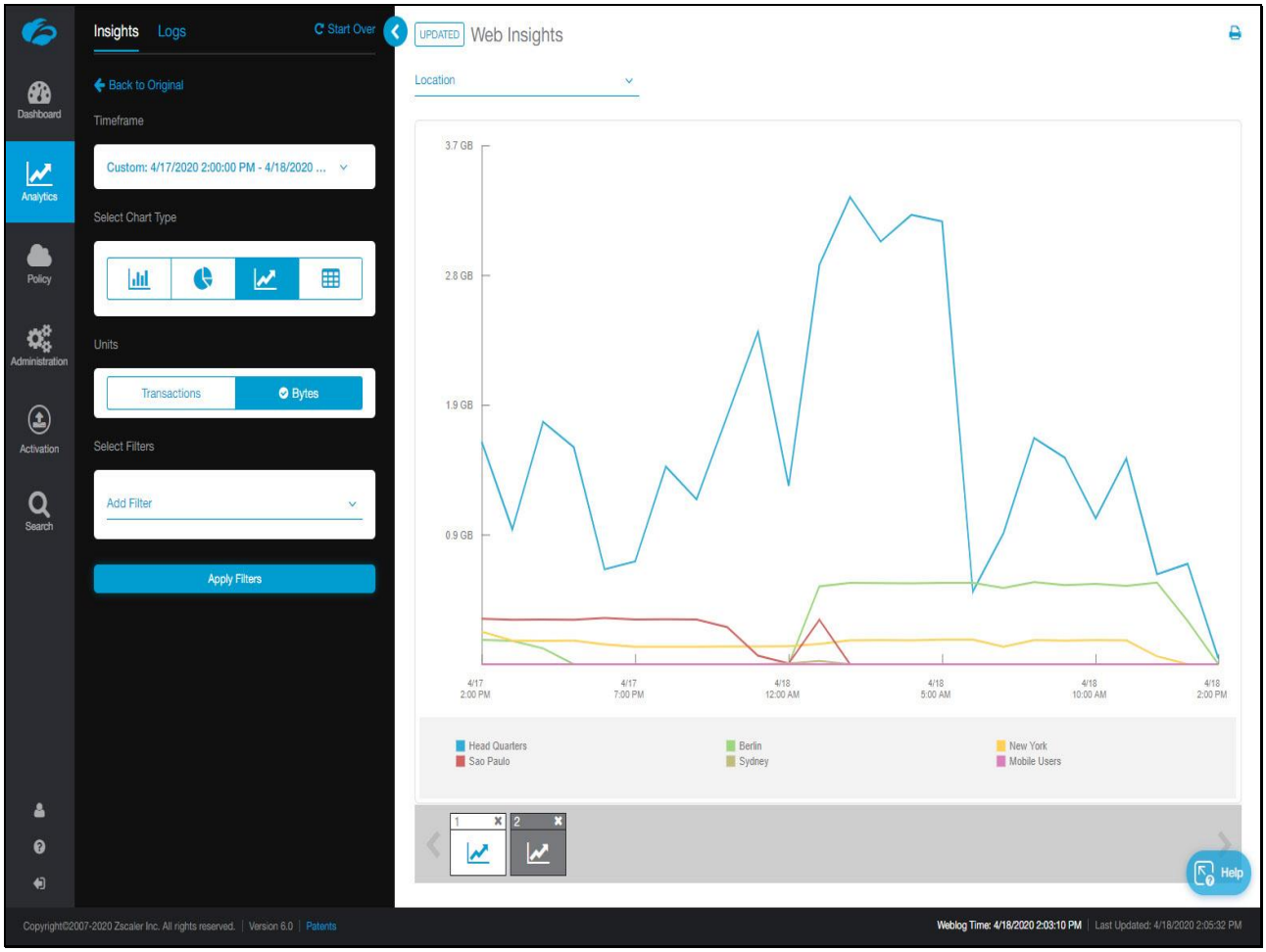
Slide 107 - Slide 107



Slide notes

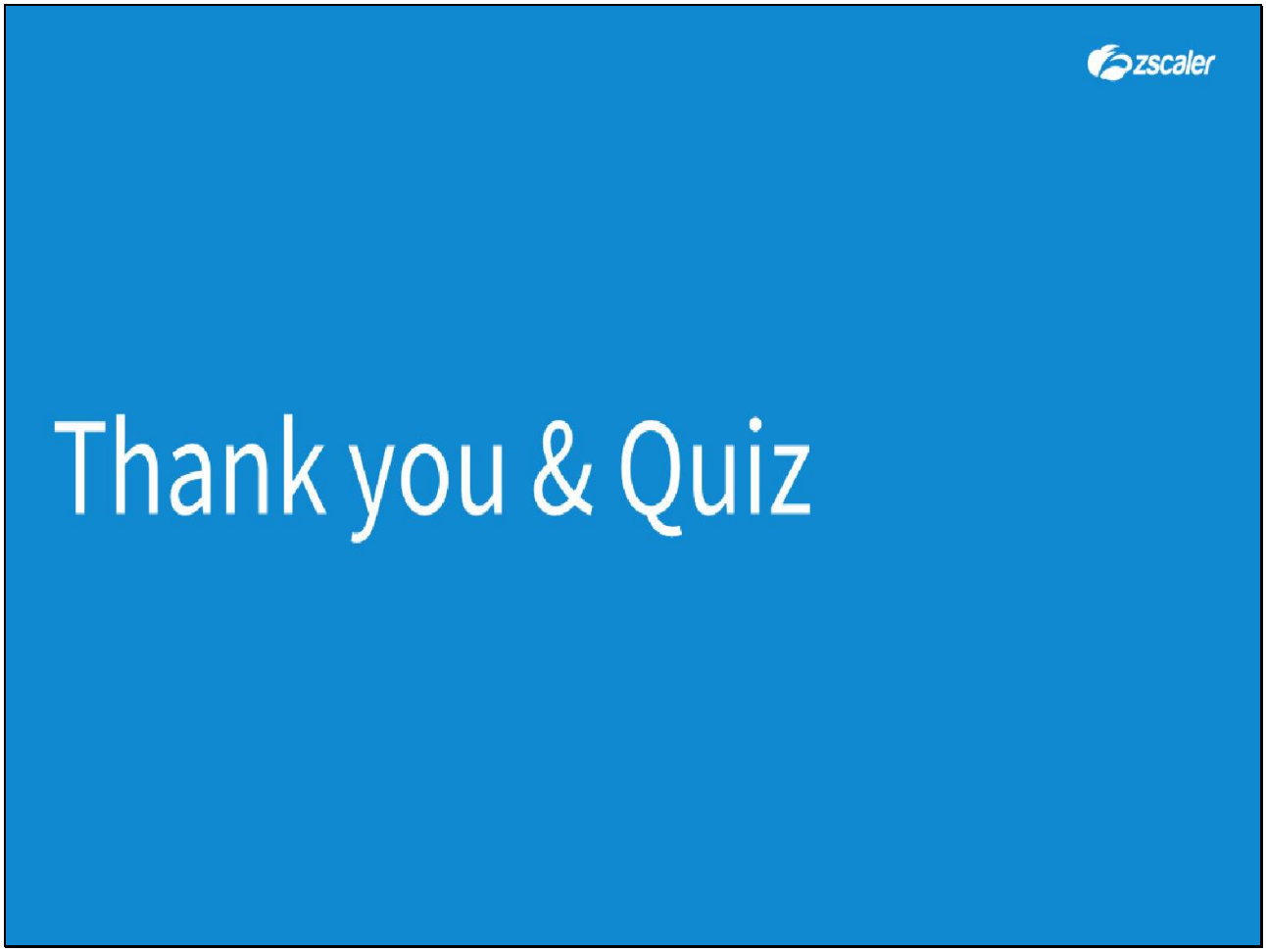
And you can see that YouTube traffic for all locations experienced a sharp drop off.

Slide 108 - Slide 108



Slide notes

Slide 109 - Thank you & Quiz



Slide notes

This concludes the Dashboard, Analytics, and Reporting module. We hope this module has been useful to you and thank you for your time. What will follow is a short quiz to test your knowledge of the material presented in this module. To take the quiz, close this module by clicking the" X " in the upper right corner of the screen then launch the quiz in the Learning portal. You may retake the quiz as many times as necessary to pass.