

Slide 1 - Dashboard and Reporting



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

Navigating the eLearning Module

The screenshot shows the Zscaler Cloud Portal Dashboard. At the top right is the Zscaler logo. On the left, there's a large blue circular chart labeled '391.3 MB 100%' and another chart labeled '16.8 K 100%'. Below these are sections for 'Cloud Application Classes', 'Top URL Categories', 'Transactions', and 'Top Users'. A blue callout points to the 'Exit' button in the top right corner of the dashboard window. Along the bottom of the dashboard are several control buttons: 'Play/Pause', 'Previous Slide', 'Next Slide', 'Fast Forward', 'Progress Bar', 'Audio On/Off', and 'Closed Captioning'. The 'Progress Bar' shows a timeline from 'Waiting Time 11:52 AM 4/4 05:02 PM Last updated 11:52 AM' to '00:17 PM'.

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

Module Agenda



- Editing Dashboards
- System defined reports
- Using the Dashboard and Reporting to track and resolve issues.

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.

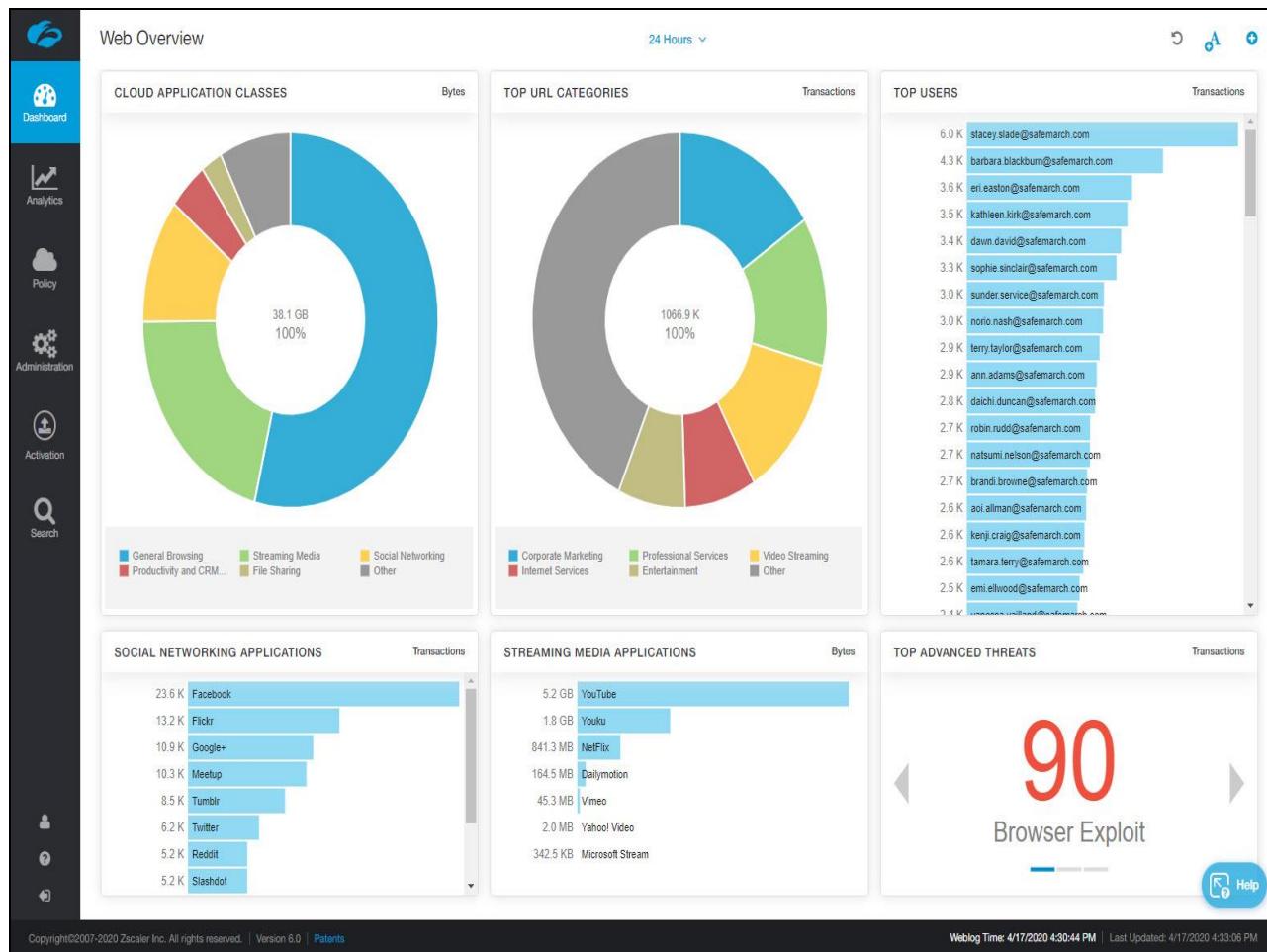
Slide 4 - Editing Dashboards



Slide notes

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

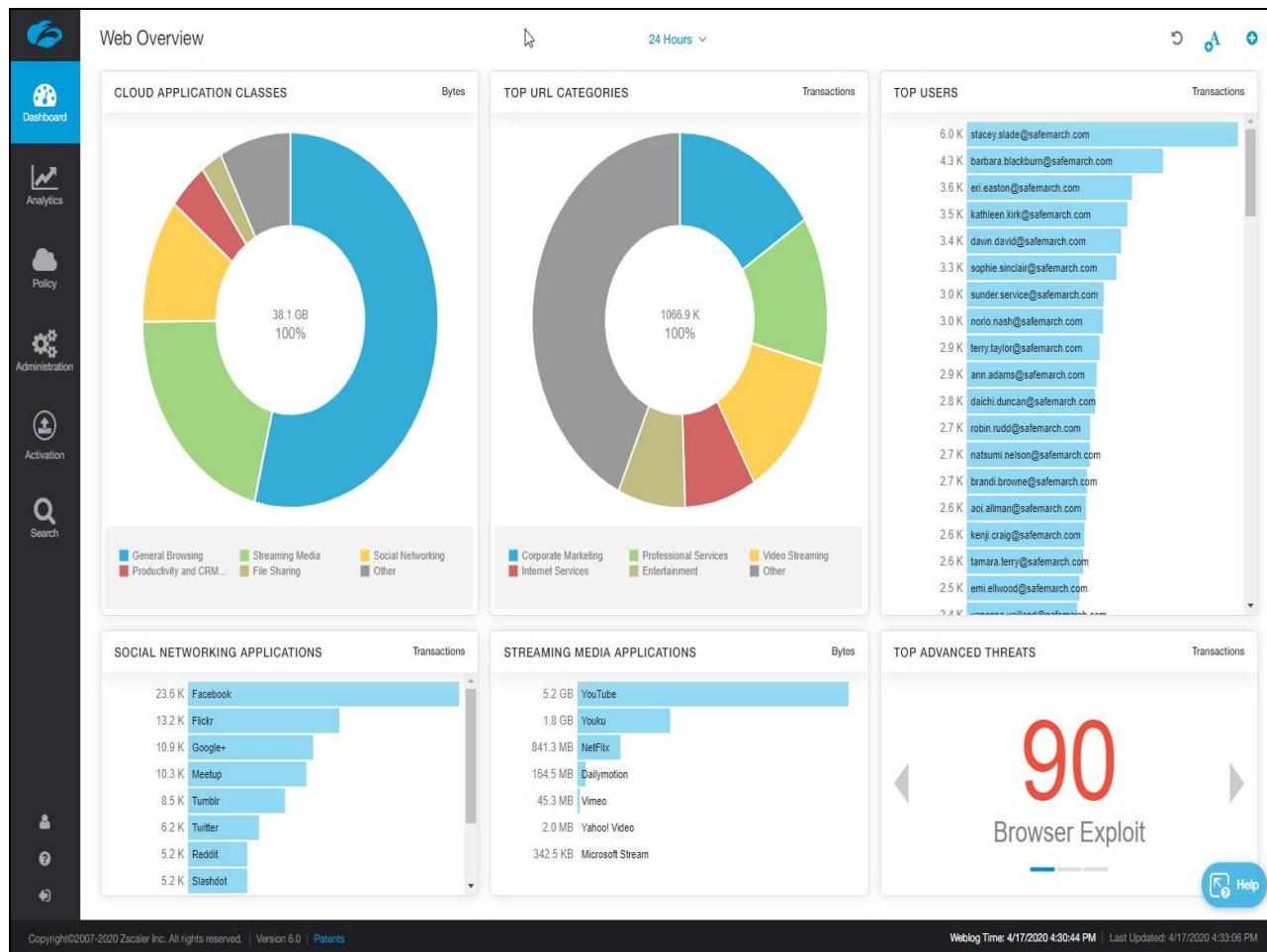
Slide 5 - Slide 5



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

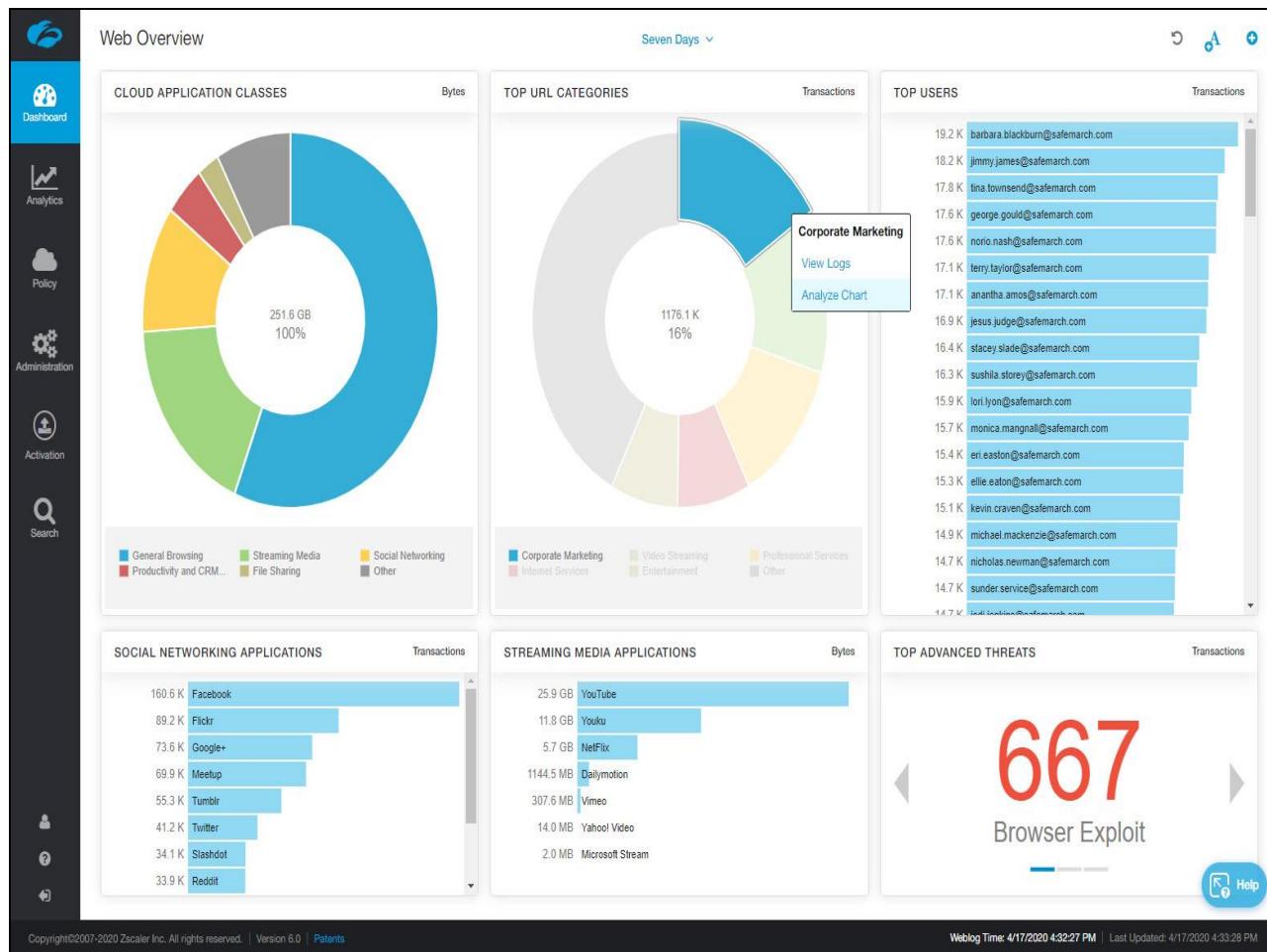
Multiple Dashboards are available, depending on which subscriptions you have purchased.

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

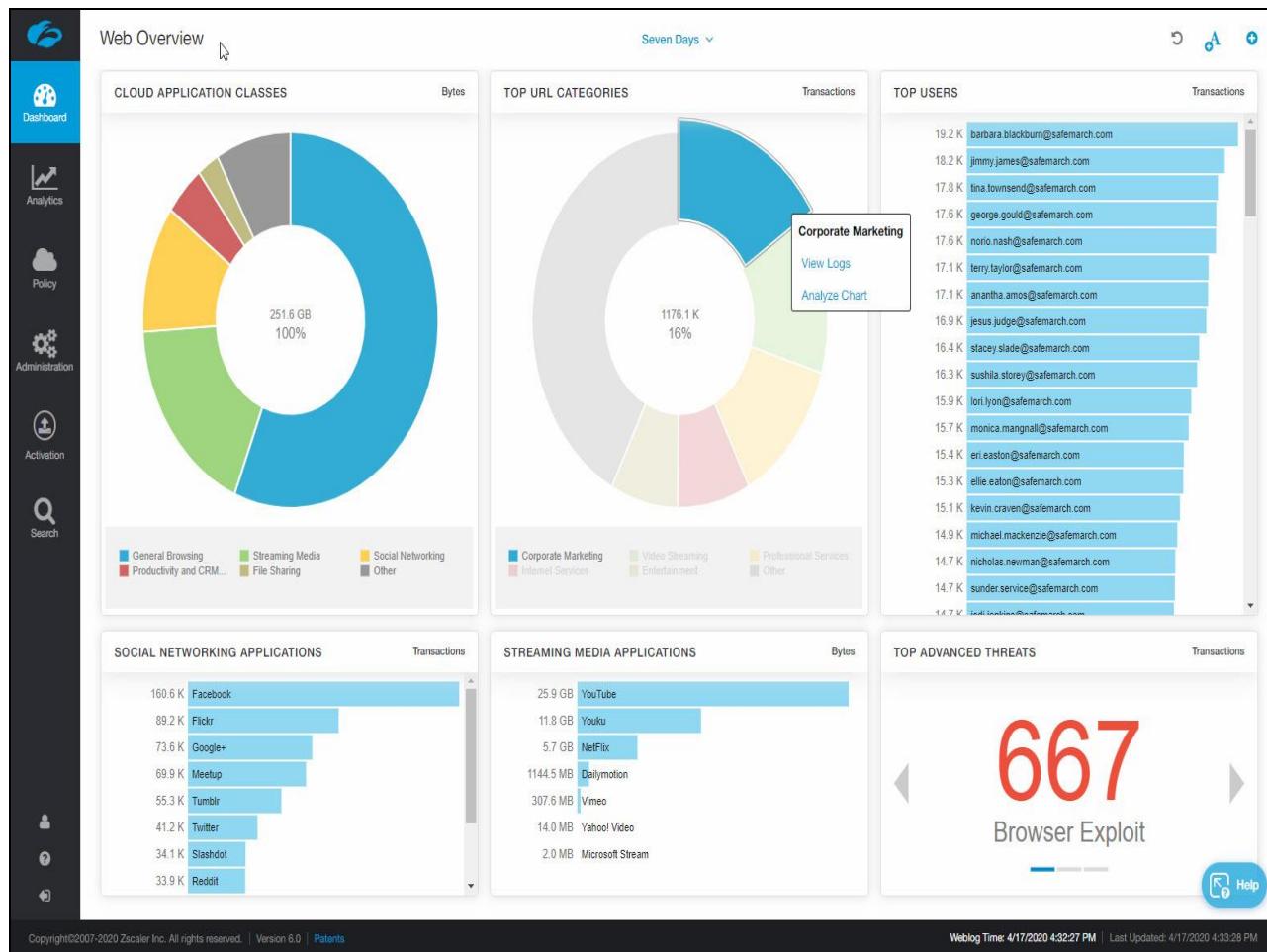


Slide notes

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

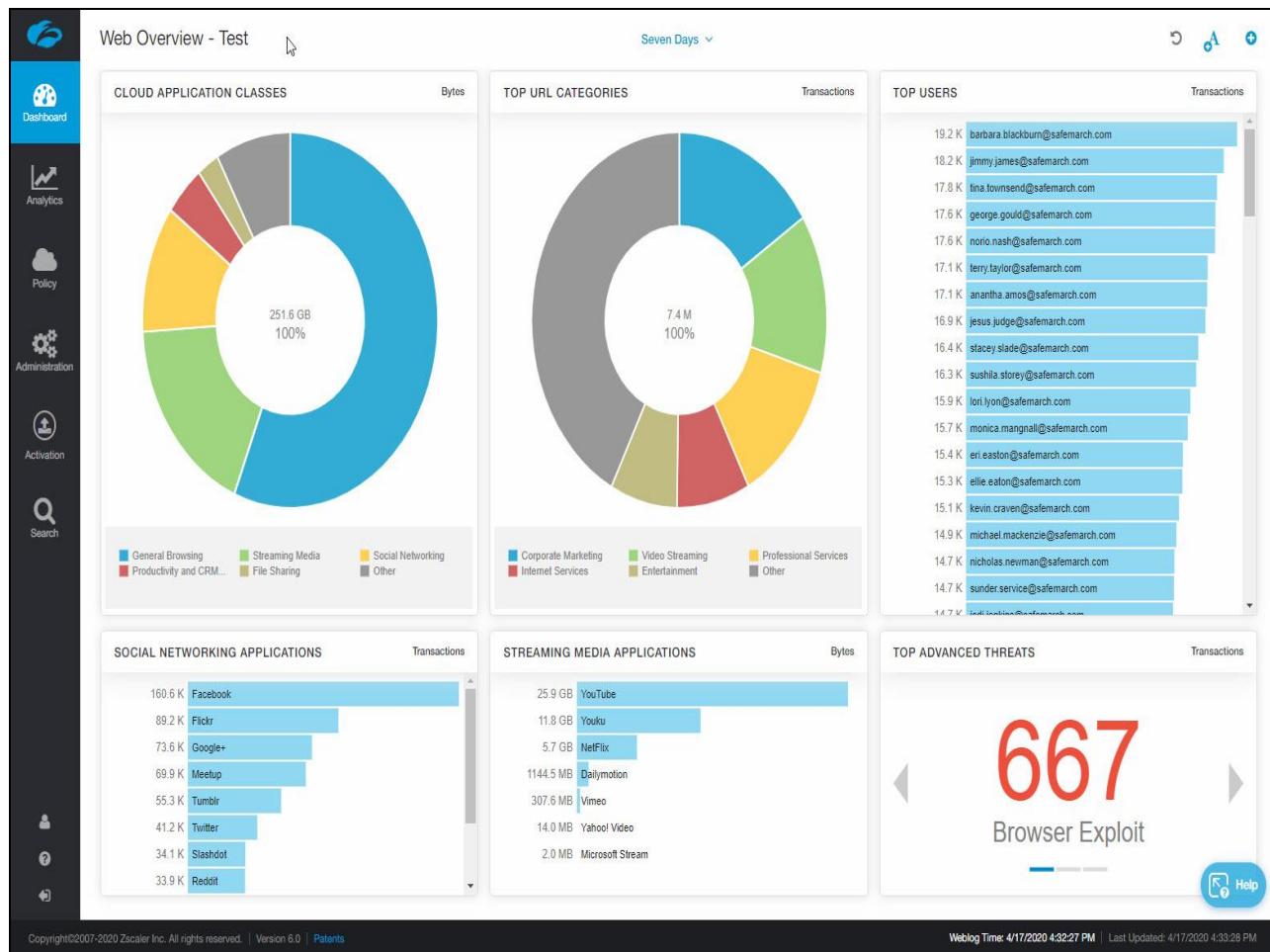


Slide notes

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.

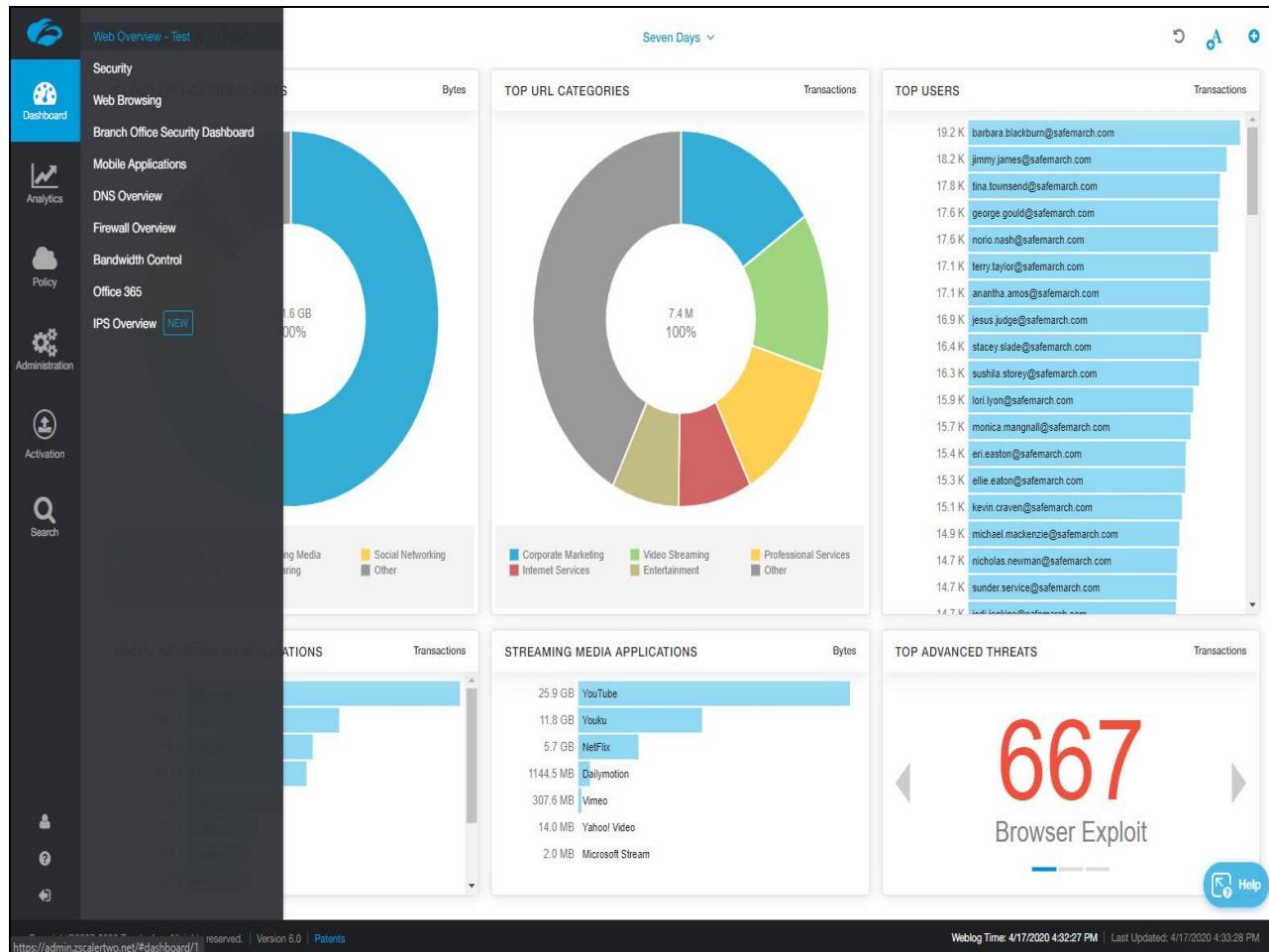
Once the dashboard name has been changed you will notice that it has also been changed in the drop-down menu of the Admin UI.

Slide 9 - Slide 9



Slide notes

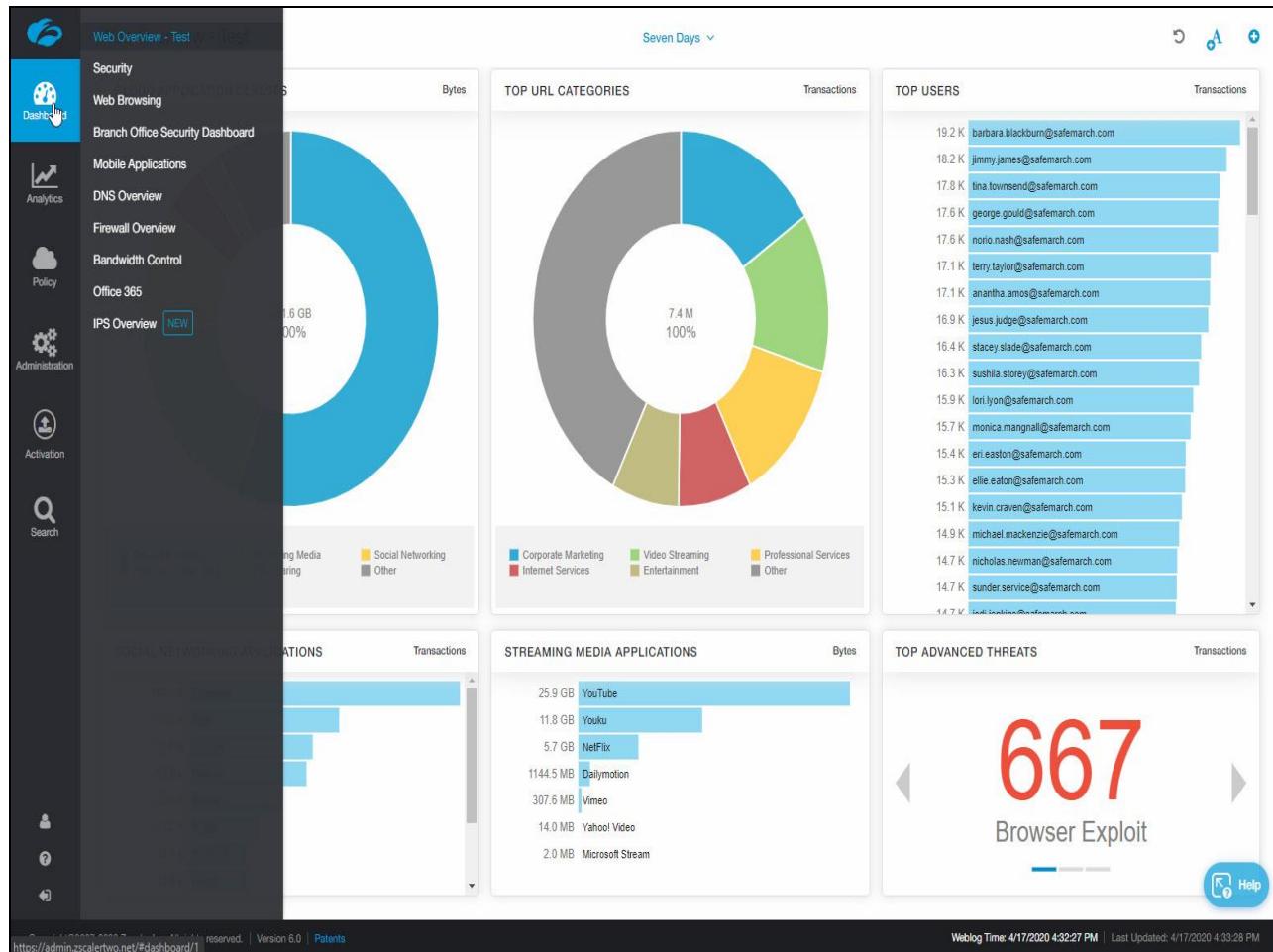
Slide 10 - Slide 10



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.

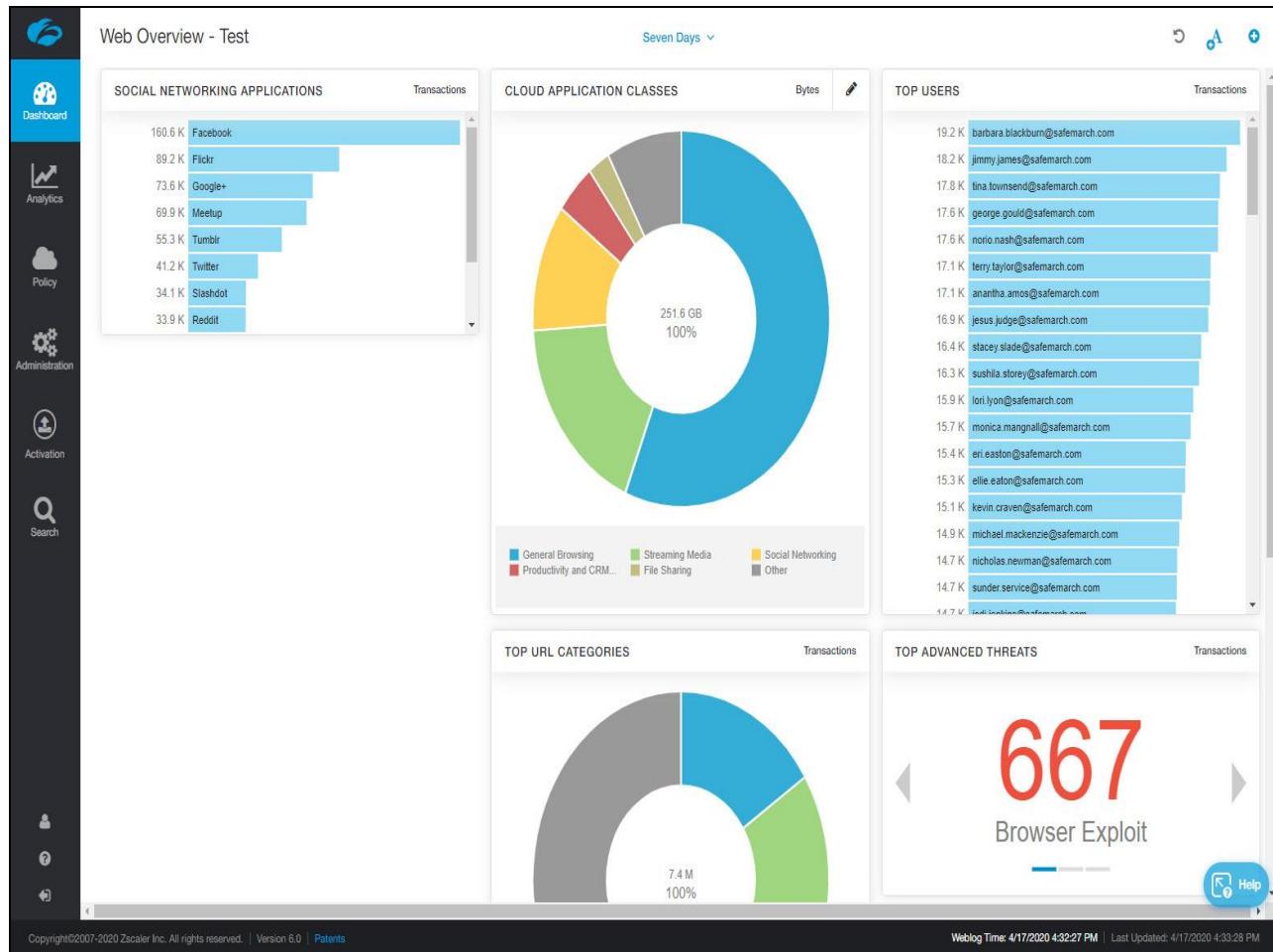
Slide 11 - Slide 11



Slide notes

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

Slide 12 - Slide 12

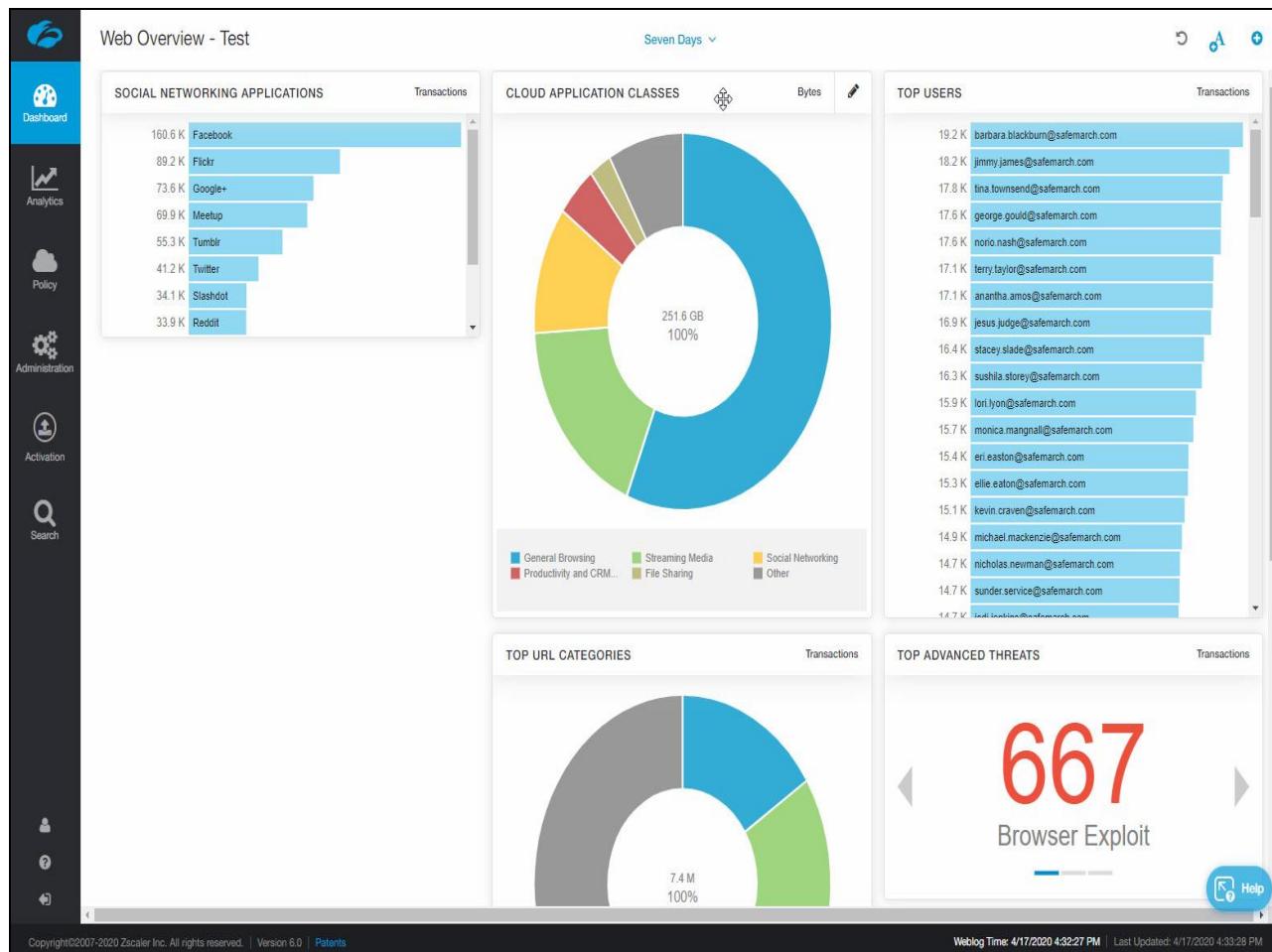


Slide notes

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

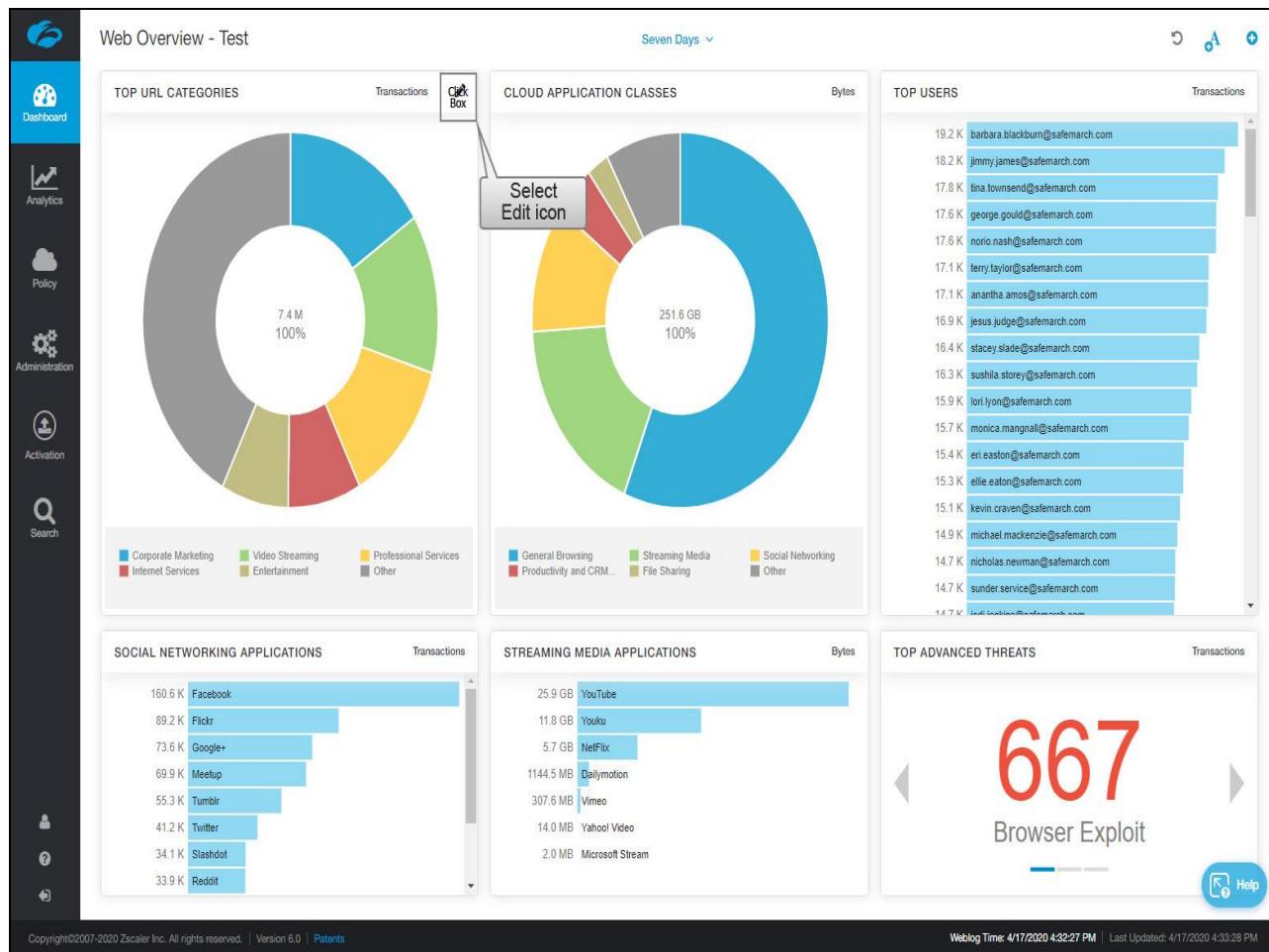
You may find that you need to fine tune the final widget placement.

Slide 13 - Slide 13



Slide notes

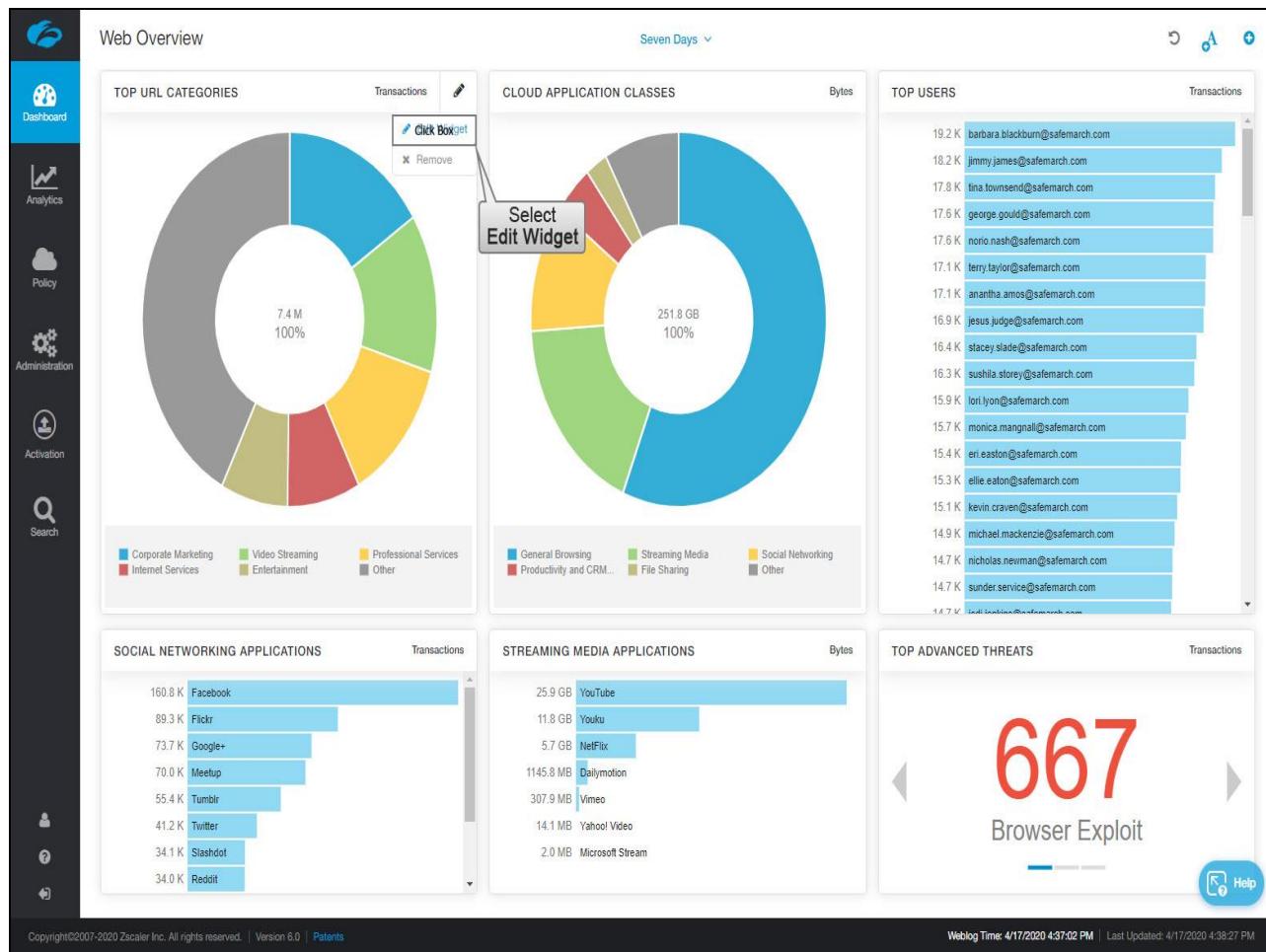
Slide 14 - Slide 14



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.

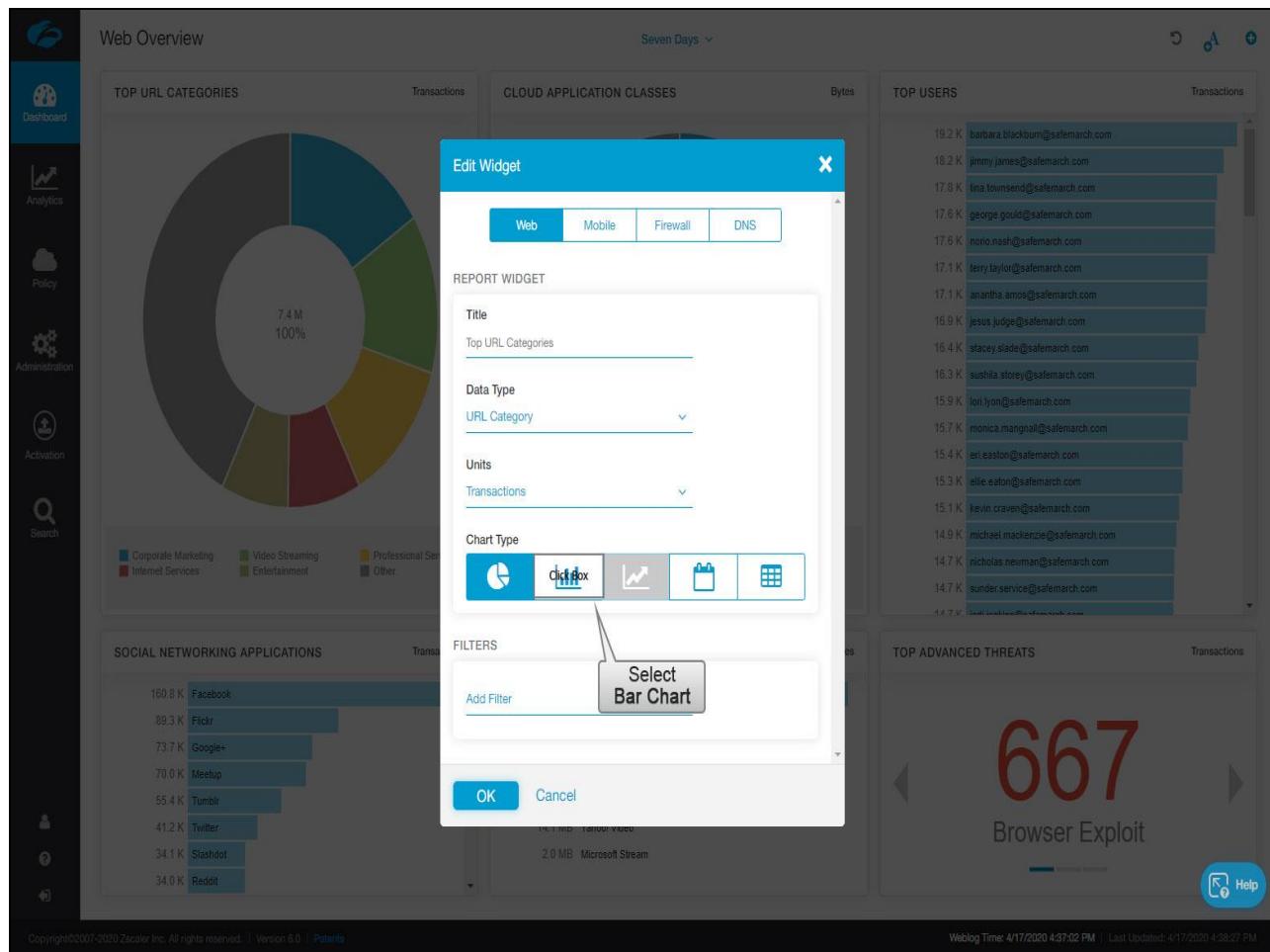
Slide 15 - Slide 15



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

The screenshot shows the Zscaler Dashboard interface with several reporting widgets:

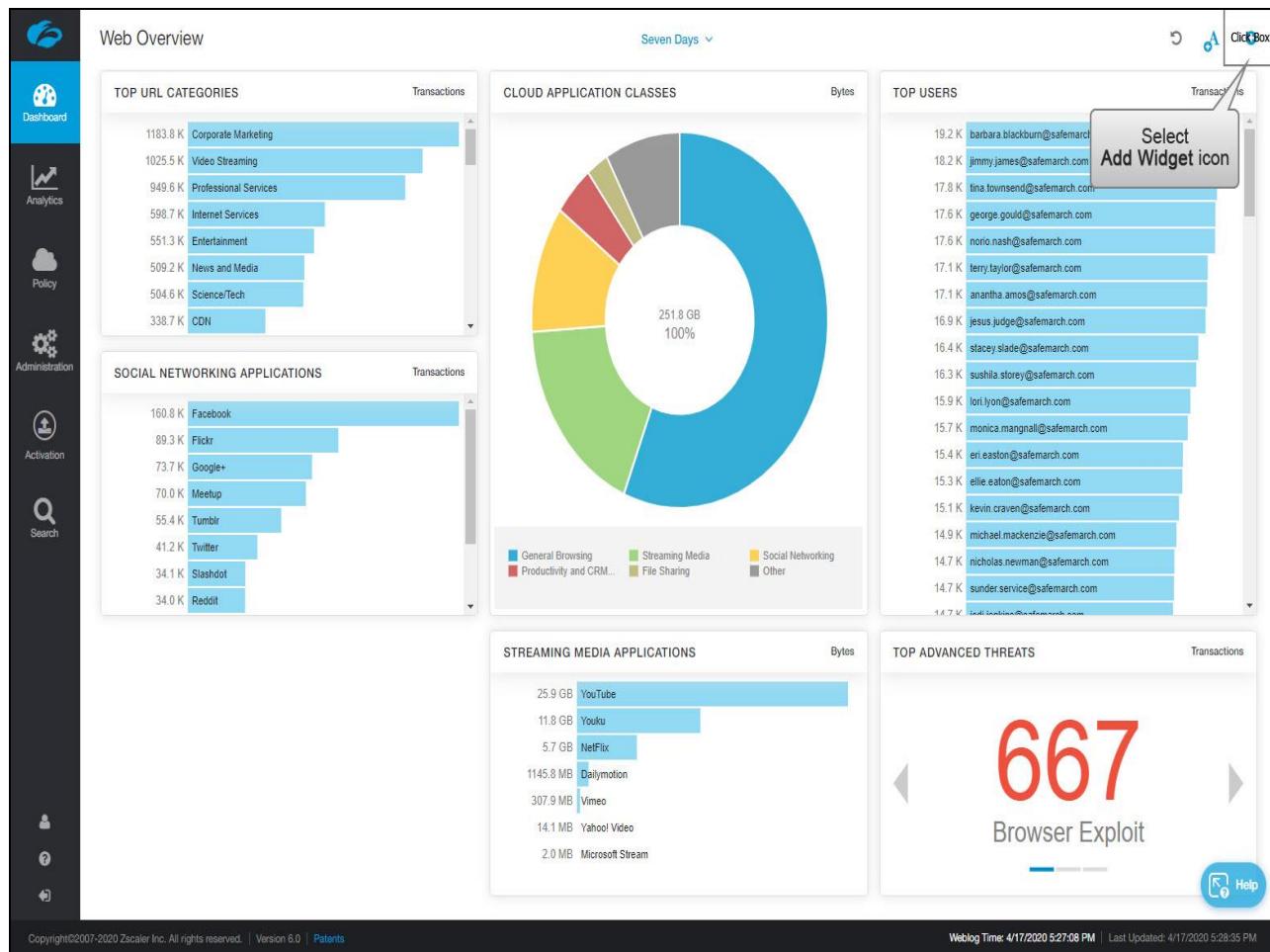
- Web Overview:** A donut chart titled "TOP URL CATEGORIES" showing transaction volumes. The chart is divided into four segments: Corporate Marketing (blue), Internet Services (red), Entertainment (green), and Other (yellow). The "Other" segment is the largest, labeled "7.4 M 100%". Below the chart is a bar chart titled "SOCIAL NETWORKING APPLICATIONS" listing platforms and their transaction counts.
- CLOUD APPLICATION CLASSES:** A bar chart titled "Transactions" showing bytes transferred for various cloud applications.
- TOP USERS:** A list of users ranked by transactions, showing email addresses and transaction counts.
- TOP ADVANCED THREATS:** A large red number "667" indicating the count of "Browser Exploit" threats.

A central modal window titled "Edit Widget" is open, allowing configuration of a "REPORT WIDGET". The "Title" is set to "Top URL Categories", "Data Type" is "URL Category", "Units" is "Transactions", and "Chart Type" is set to a donut chart icon. A "FILTERS" section contains a "Select OK" button and a "Cancel" button. At the bottom of the modal, there are "OK Box" and "Cancel" buttons.

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

The screenshot shows the Zscaler Dashboard interface. A central modal window titled "New Widget" is open, allowing users to create a new report widget. The modal includes fields for "Title" (set to "New Widget"), "Data Type" (set to "Overall Traffic"), "Units" (set to "Transactions"), and a "Chart Type" section with a bar chart icon selected. Below the chart type are five other chart type icons: bar, line, area, pie, and grid. The "FILTERS" section contains a dropdown menu with "Add Filter". At the bottom of the modal are "OK" and "Cancel" buttons. The background of the dashboard shows various data panels: "TOP URL CATEGORIES", "CLOUD APPLICATION CLASSES", "TOP USERS", and "TOP ADVANCED THREATS" (displaying "667 Browser Exploit"). The left sidebar contains navigation links for Dashboard, Analytics, Policy, Administration, Activation, and Search.

Slide notes

Provide a name for the new widget.

Slide 20 - Slide 20

The screenshot displays a complex dashboard interface with several data panels and a central configuration window.

- Left Sidebar:** Contains icons for Dashboard, Analytics, Policy, Administration, Activation, and Search.
- Top Navigation:** Shows "Seven Days" and a dropdown menu.
- Web Overview:** A large panel containing three main sections: TOP URL CATEGORIES, CLOUD APPLICATION CLASSES, and TOP USERS.
- TOP URL CATEGORIES:** Shows counts for Corporate Marketing, Video Streaming, Professional Services, Internet Services, Entertainment, News and Media, ScienceTech, and CDN.
- CLOUD APPLICATION CLASSES:** Shows counts for Facebook, Flickr, Google+, Meetup, Tumblr, Twitter, Slashdot, and Reddit.
- TOP USERS:** A list of users with their transaction counts, such as barbara.blackburn@safemarch.com (19.2 K), jimmy.james@safemarch.com (18.2 K), lma.townsend@safemarch.com (17.8 K), etc.
- New Widget:** A modal window titled "New Widget" with tabs for Web, Mobile, Firewall, and DNS. It includes fields for Title (Web Action - Allow / Block), Data Type (Overall Traffic), Units (Transactions), and Chart Type (Bar, Line, Area, Calendar). It also has a FILTERS section with an "Add Filter" button and OK/Cancel buttons.
- TOP ADVANCED THREATS:** A summary section showing a large red number "667" and the text "Browser Exploit".
- Bottom Footer:** Includes copyright information (Copyright 2007-2020 Zscaler Inc. All rights reserved.), version (Version 6.0), patents link, help icon, and system status (Weblog Time: 4/17/2020 5:27:08 PM | Last Updated: 4/17/2020 5:29:05 PM).

Slide notes

Slide 21 - Slide 21

The screenshot shows the Zscaler Dashboard interface. In the center, a modal window titled "New Widget" is open. The "Web" tab is selected. Inside the modal, there are fields for "Title" (set to "Web Action - Allow / Block") and "Data Type" (set to "Overall Traffic"). A callout bubble points to the "Data Type" dropdown menu, which is currently set to "Click Box". Other options in the dropdown include "Transactions" and "Bytes". Below the dropdown are sections for "Units" (set to "Transactions") and "Chart Type" (with three chart icons: donut, bar, and line). At the bottom of the modal are "OK" and "Cancel" buttons. The background of the dashboard shows various reports: "TOP URL CATEGORIES", "CLOUD APPLICATION CLASSES", "TOP USERS", and "TOP ADVANCED THREATS" (showing 667 Browser Exploit). The left sidebar contains navigation links for Dashboard, Analytics, Policy, Administration, Activation, and Search.

Slide notes

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

Slide 22 - Slide 22

The screenshot shows a 'New Widget' dialog box centered over a dark-themed dashboard. The dashboard features several cards:

- Web Overview:** Includes 'TOP URL CATEGORIES' (Corporate Marketing, Video Streaming, Professional Services, Internet Services, Entertainment, News and Media, ScienceTech, CDN) and 'SOCIAL NETWORKING APPLICATIONS' (Facebook, Flickr, Google+, Meetup, Tumblr, Twitter, Slashdot, Reddit).
- CLOUD APPLICATION CLASSES:** Shows transaction counts for various applications.
- TOP USERS:** Lists users with their transaction counts and email addresses.
- TOP ADVANCED THREATS:** Displays a large number '667' and the category 'Browser Exploit'.

The 'New Widget' dialog has tabs for Web, Mobile, Firewall, and DNS. It includes fields for Title (Web Action - Allow / Block), Data Type (Overall Traffic selected), and a search bar. A sidebar lists categories like Overall Traffic, Protocol, Sandbox, Sandbox Action, and Secure Browsing Class. At the bottom are OK and Cancel buttons.

Slide notes

Slide 23 - Slide 23

The screenshot shows the Zscaler Dashboard interface. A central modal window titled "New Widget" is open, allowing users to create a custom report. The modal includes tabs for "Web", "Mobile", "Firewall", and "DNS". Below the tabs, there's a "REPORT WIDGET" section with a "Title" field containing "Web Action - Allow / Block". Under "Data Type", a dropdown menu is set to "Overall Traffic" and includes options like "Secure Browsing Status", "Secure Browsing Type", "Server Side Cipher", "Server Side TLS Version", and "Social Networking Activity". At the bottom of the modal are "OK" and "Cancel" buttons. The background of the dashboard features several reporting sections: "TOP URL CATEGORIES", "CLOUD APPLICATION CLASSES", "TOP USERS", and "TOP ADVANCED THREATS". The "TOP USERS" section lists numerous email addresses with their transaction counts, such as barbara.blackburn@safemarch.com (19.2 K) and jimmy.james@safemarch.com (18.2 K). The "TOP ADVANCED THREATS" section displays a large red number "667" and the text "Browser Exploit". The bottom of the screen includes copyright information ("Copyright 2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents") and a help icon.

Slide notes

Slide 24 - Slide 24

The screenshot shows the Zscaler Dashboard interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area has several cards: 'TOP URL CATEGORIES', 'CLOUD APPLICATION CLASSES', 'TOP USERS', and 'TOP ADVANCED THREATS'. The 'TOP ADVANCED THREATS' card displays a large red number '667' and the text 'Browser Exploit'. In the center, a modal window titled 'New Widget' is open. It has tabs for 'Web', 'Mobile', 'Firewall', and 'DNS', with 'Web' selected. Under 'REPORT WIDGET', there's a 'Title' input field containing 'Web Action - Allow / Block'. A 'Data Type' dropdown is set to 'Overall Traffic', with other options like 'URL Class', 'URL Super Category', and 'User' available. A search bar with 'Search...' placeholder text is also present. Below these, a 'Web Action' dropdown is set to 'Click Box', with other options like 'Webmail Activity' visible. At the bottom of the modal are 'OK' and 'Cancel' buttons. A callout bubble points to the 'Web Action' dropdown with the text 'Select Web Action'.

Slide notes

Select “Web Action”.

Slide 25 - Slide 25

The screenshot shows the Zscaler Dashboard interface. In the center, a modal window titled "New Widget" is open, allowing users to configure a report widget. The "Chart Type" section is highlighted, showing five options: Line chart (selected), Bar chart, Map, Calendar, and Grid. A callout box points to the "Line chart" icon with the instruction "Select Line Chart icon". The background of the dashboard displays various performance metrics and user activity lists.

Slide notes

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

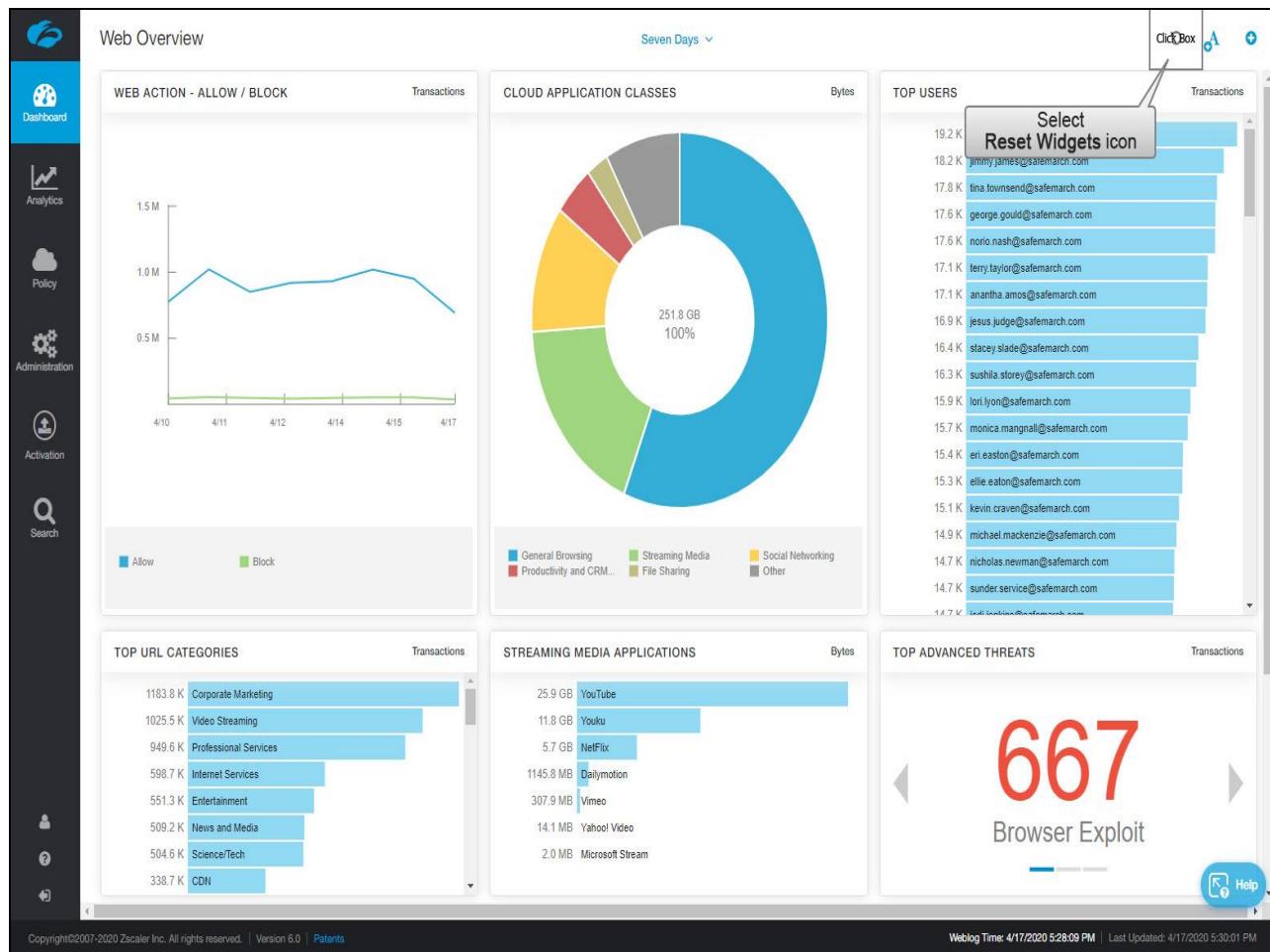
Slide 26 - Slide 26

The screenshot shows the Zscaler Dashboard interface. A central modal window titled "New Widget" is open, allowing users to configure a new report widget. The modal includes tabs for "Web", "Mobile", "Firewall", and "DNS", with "Web" currently selected. Inside the modal, there are sections for "REPORT WIDGET" (Title: "Web Action - Allow / Block", Data Type: "Web Action", Units: "Transactions"), "CHART TYPE" (with five chart icons), and "FILTERS" (with an "Add Filter" button and a "Select OK" button). The background of the dashboard shows various performance metrics and threat reports, such as "TOP URL CATEGORIES", "CLOUD APPLICATION CLASSES", "TOP USERS", and "TOP ADVANCED THREATS". The "TOP USERS" panel lists numerous email addresses with their transaction counts, and the "TOP ADVANCED THREATS" panel displays a large red number "667" followed by the text "Browser Exploit".

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

The screenshot shows the Zscaler Dashboard interface with various charts and tables. A central modal dialog box is displayed, asking for confirmation to reset the dashboard to its default settings. The dialog includes a 'Select OK' button highlighted with a blue box and a 'Cancel' button.

Reset to Default

Are you sure you want to reset this dashboard to its default settings?
This action cannot be undone.

Select OK Cancel

Web Overview

CLOUD APPLICATION CLASSES

TOP USERS

TOP URL CATEGORIES

STREAM APPLICATIONS

TOP ADVANCED THREATS

667 Browser Exploit

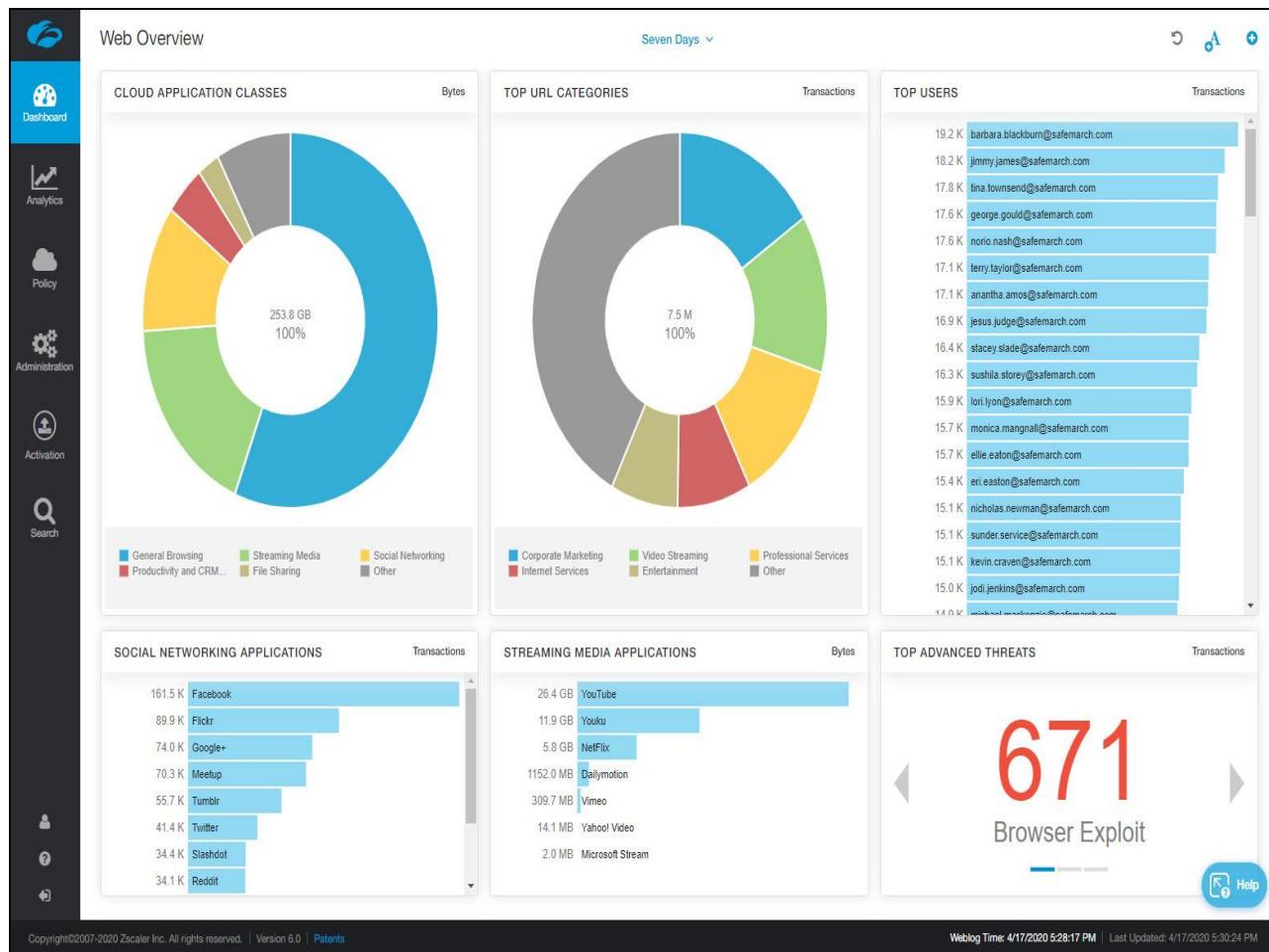
Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | [Privacy](#)

Weblog Time: 4/17/2020 5:28:09 PM | Last Updated: 4/17/2020 5:30:01 PM

Slide notes

Then read the warning message and click OK.

Slide 29 - Slide 29



Slide notes

Slide 30 - System defined reports



System defined reports

- Executive Report
- Industry Peer Comparison Report

Slide notes

As a new Zscaler administrator it is important for you to quickly assess 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 -

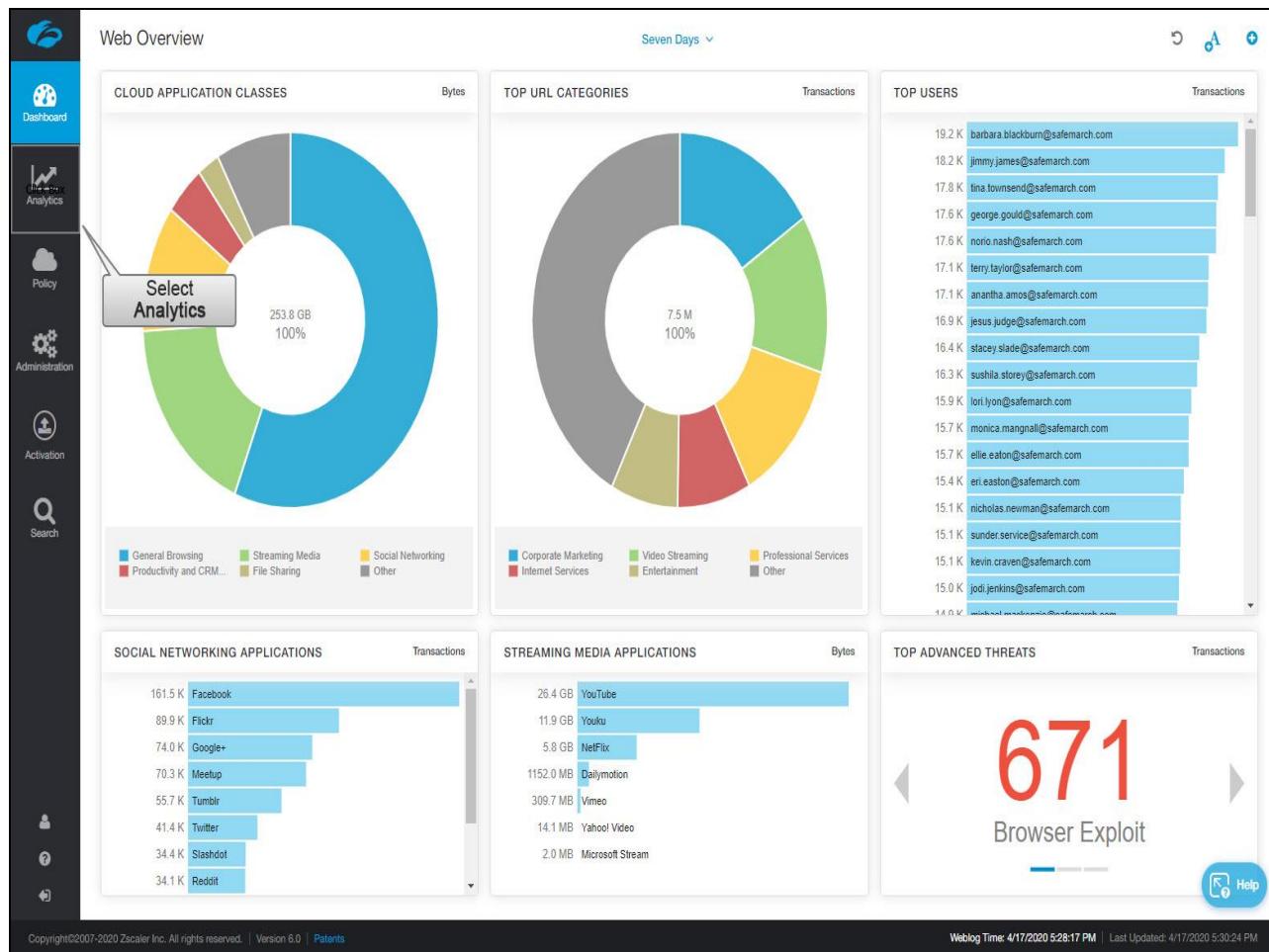
Executive Report



Executive Report

Slide notes

Slide 32 - Slide 32



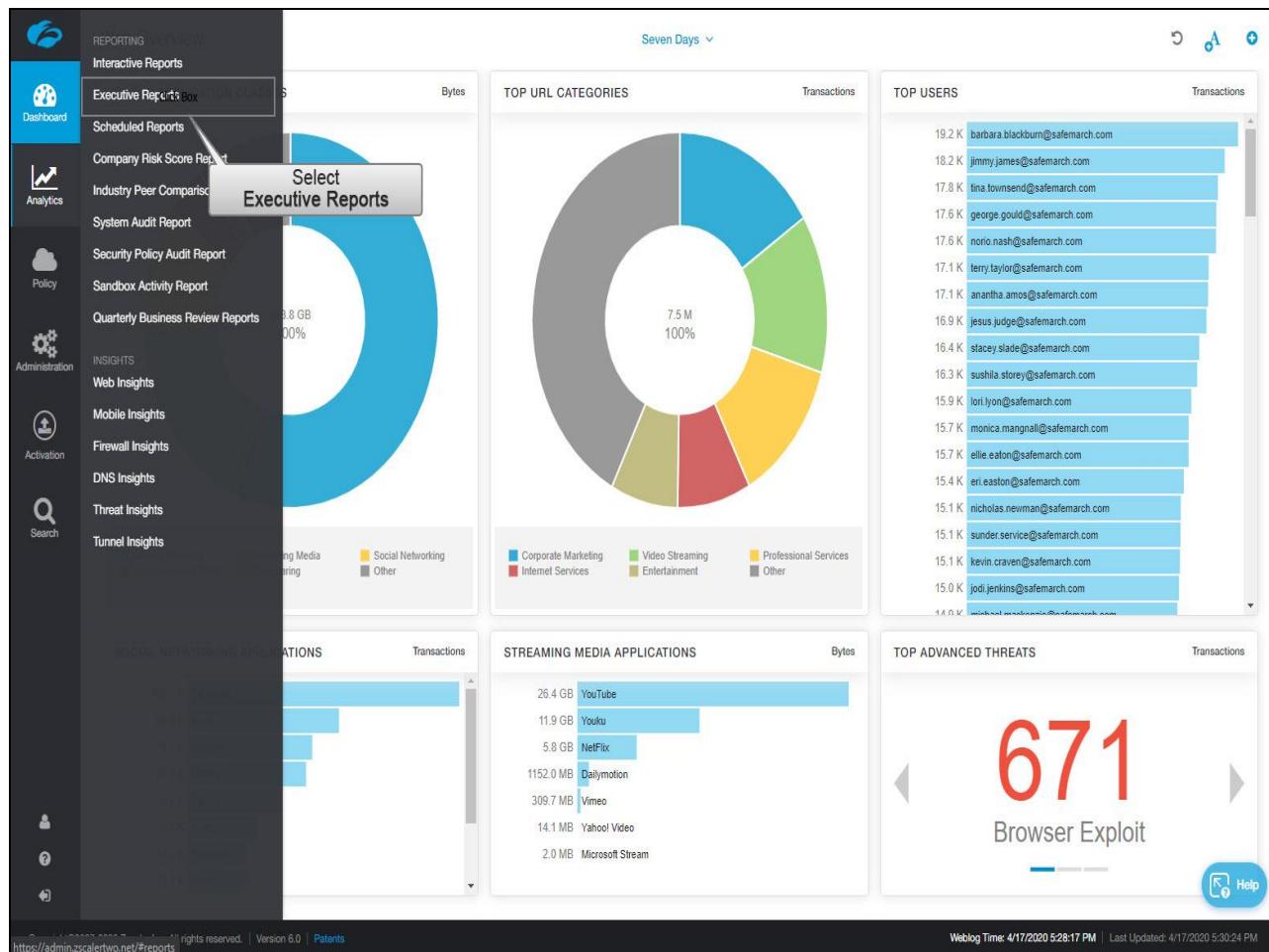
Slide notes

The first report you want to review, once Zscaler has been inline and examining your organization's 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

The screenshot shows the Zscaler Dashboard interface. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area has a blue header bar with the text "Safemarch" and "Internet Security Update". A callout box points to a dropdown menu labeled "Select time period drop-down" which is currently set to "Current Month: Click Box - 4/17/2020". The central part of the dashboard features a large blue banner with the text "Zscaler protected you from 1,035,466 potentially harmful activities." Below this are two sections: "Protected Locations" (Safemarch has protected 6 locations including sublocations) and "Protected Internet Traffic" (Zscaler processed 24.2 M total internet transactions from 4/1/2020 to 4/17/2020). At the bottom, there are three cards: "Overall Protection" (1,035,466), "Threats Blocked" (37,630), and "Policy Violations" (997,836). Each card includes a horizontal bar chart comparing "Your Score" and "Cloud Averages". The footer contains copyright information, a help link, and a timestamp.

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | [Patents](#)

Weblog Time: 4/17/2020 5:28:17 PM | Last Updated: 4/17/2020 5:30:24 PM

Help

Slide notes

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

Slide 35 - Slide 35

The screenshot shows the Zscaler Safemarch dashboard. On the left, a vertical sidebar lists navigation options: Executive Reports, Dashboard, Analytics, Policy, Administration, Activation, and Search. A dropdown menu for date selection is open, showing options like Current Day, Current Week, Current Month (which is selected), Previous Day, Previous Week, Previous Month (highlighted with a red box and a callout 'Select Previous Month'), and Custom. The main content area has a blue header bar with the text 'Safemarch' and 'Internet Security Update'. Below this, a large white section displays the message 'Zscaler protected you from 1,035,466 potentially harmful activities.' In the bottom right corner of this section, there is a small 'Help' button icon. To the left of the main message, there are two sections: 'Protected Locations' (Safemarch has protected 6 locations including sublocations) and 'Protected Internet Traffic' (Zscaler processed 21.2 M total internet transactions from 4/1/2020 to 4/17/2020). At the bottom of the dashboard, there are three performance boxes: 'Overall Protection' (1,035,466), 'Threats Blocked' (37,630), and 'Policy Violations' (997,836). Each box includes a horizontal bar chart comparing 'Your Score' (green/red/orange) against 'Cloud Averages' (grey).

Slide notes

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

Select Previous Month.

Slide 36 - Slide 36

The screenshot shows the Zscaler dashboard interface. On the left, a vertical sidebar contains icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area has a blue header bar with the text "Safemarch" and "Internet Security Update". Below this, a large blue section displays the headline: "Zscaler protected you from 1,035,466 potentially harmful activities." To the left of this headline is a dropdown menu for selecting time periods: Current Day, Current Week, Current Month (which is selected), Previous Day, Previous Week, Previous Month, and Custom. To the right are links for "Schedule" and "Print". In the center, there are two sections: "Protected Locations" (Safemarch has protected 6 locations including sublocations) and "Protected Internet Traffic" (Zscaler processed 24.2 M total internet transactions from 4/1/2020 to 4/17/2020). At the bottom, three cards provide detailed statistics: Overall Protection (1,035,466), Threats Blocked (37,630), and Policy Violations (997,836). Each card includes a horizontal bar chart comparing "Your Score" (green) and "Cloud Averages" (black). The footer contains copyright information ("Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents") and a timestamp ("Weblog Time: 4/17/2020 5:28:17 PM | Last Updated: 4/17/2020 5:30:24 PM"). A "Help" button is located in the bottom right corner.

Slide notes

Slide 37 - Slide 37

The screenshot shows a web-based dashboard titled "Safemarch" under "Internet Security Update". The main headline reads: "Zscaler protected you from 3,131,056 potentially harmful activities." Below this, there are two sections: "Protected Locations" (7 locations) and "Protected Internet Traffic" (55M transactions from 3/1/2020 to 3/31/2020). At the bottom, three performance metrics are displayed: Overall Protection (3,131,056), Threats Blocked (104,770), and Policy Violations (3,026,286). Each metric includes a comparison bar chart showing "Your Score" versus "Cloud Averages". The left sidebar contains links to "Executive Reports", "Dashboard", "Analytics", "Policy", "Administration", "Activation", and "Search". The bottom footer includes copyright information, version details, and a help link.

Executive Reports

Previous Month: 3/1/2020 - 3/31/2020

Schedule Print

Safemarch | Internet Security Update

Zscaler protected you from 3,131,056 potentially harmful activities.

Protected Locations
Safemarch has protected 7 locations including sublocations

Protected Internet Traffic
Zscaler processed 55 M total internet transactions from 3/1/2020 to 3/31/2020

Overall Protection
3,131,056

Threats Blocked
104,770

Policy Violations
3,026,286

5.69% Your Score 6.12% Cloud Averages

0.19% Your Score 0.11% Cloud Averages

5.50% Your Score 6.01% Cloud Averages

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents

Weblog Time: 4/17/2020 5:28:17 PM | Last Updated: 4/17/2020 5:30:24 PM

Help

Slide notes

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

Slide 38 - Slide 38

The screenshot shows the Zscaler Safemarch dashboard. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area has a blue header with the text "Safemarch" and "Internet Security Update". The central message is "Zscaler protected you from 3,131,056 potentially harmful activities." Below this are two sections: "Protected Locations" (7 locations) and "Protected Internet Traffic" (55M transactions). At the bottom, there are three boxes: "Overall Protection" (3,131,056), "Threats Blocked" (104,770), and "Policy Violations" (3,026,286). Each box includes a horizontal bar chart comparing "Your Score" and "Cloud Averages". The bottom of the screen shows copyright information and a help icon.

Executive Reports

Previous Month: 3/1/2020 - 3/31/2020

Schedule Print

Safemarch | Internet Security Update

Zscaler protected you from
3,131,056
potentially harmful activities.

Protected Locations
Safemarch has protected 7 locations including sublocations

Protected Internet Traffic
Zscaler processed 55 M total internet transactions from 3/1/2020 to 3/31/2020

Overall Protection
3,131,056

Threats Blocked
104,770

Policy Violations
3,026,286

5.69% Your Score 6.12% Cloud Averages

0.19% Your Score 0.11% Cloud Averages

5.50% Your Score 6.01% Cloud Averages

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents

Help

Weblog Time: 4/17/2020 5:28:17 PM | Last Updated: 4/17/2020 5:30:24 PM

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

The screenshot shows the Zscaler Safemarch dashboard. On the left is a vertical navigation bar with icons for Executive Reports, Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area has a blue header with the text "Safemarch" and "Internet Security Update". The main message is "Zscaler protected you from 3,131,056 potentially harmful activities." Below this are two sections: "Protected Locations" (7 locations) and "Protected Internet Traffic" (55M transactions). At the bottom, there are three boxes: "Overall Protection" (3,131,056), "Threats Blocked" (104,770), and "Policy Violations" (3,026,286). Each box includes a horizontal bar chart comparing "Your Score" and "Cloud Averages". The footer contains copyright information, a help icon, and a timestamp.

Executive Reports

Previous Month: 3/1/2020 - 3/31/2020

Schedule Print

Safemarch | Internet Security Update

Zscaler protected you from
3,131,056
potentially harmful activities.

Protected Locations
Safemarch has protected 7 locations including sublocations

Protected Internet Traffic
Zscaler processed 55 M total internet transactions from 3/1/2020 to 3/31/2020

Overall Protection
3,131,056

Threats Blocked
104,770

Policy Violations
3,026,286

5.69% Your Score 6.12% Cloud Averages

0.19% Your Score 0.11% Cloud Averages

5.50% Your Score 6.01% Cloud Averages

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents

Help

Weblog Time: 4/17/2020 5:28:17 PM | Last Updated: 4/17/2020 5:30:24 PM

Slide notes

Slide 40 - Slide 40

The screenshot shows the Zscaler Executive Reports dashboard. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area features a large blue header with the text "Zscaler protected you from 3,131,056 potentially harmful activities." Below this, two sections provide detailed statistics: "Protected Locations" (Safemarch has protected 7 locations including sublocations) and "Protected Internet Traffic" (Zscaler processed 55 M total internet transactions from 3/1/2020 to 3/31/2020). The central part of the dashboard displays three performance metrics in boxes: Overall Protection (3,131,056), Threats Blocked (104,770), and Policy Violations (3,026,286). Each metric includes a comparison bar chart showing "Your Score" versus "Cloud Averages". At the bottom, copyright information (Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents) and system status (Weblog Time: 4/17/2020 5:28:17 PM | Last Updated: 4/17/2020 5:30:24 PM) are visible.

Slide notes

Slide 41 - Slide 41

The screenshot shows the Zscaler Dashboard interface. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area is titled "Executive Reports" and shows a summary of blocked threats. A callout box highlights the detection and blocking of browser exploits. Below this, there's a note about botnets and a link to help.

Advanced Threats Blocked

5,654	Browser Exploit
3,725	Phishing
1,802	Cross-site Scripting

We detected and blocked 5654 instances of browser exploit that could have infected your users.

We didn't detect any attempts by botnets to "call home."

Without Zscaler, we find that an organization can have 8-10% of its PCs infected with botnets. Companies must operate under the assumption that you have been breached but you just haven't detected it yet. Now the question becomes, how can you minimize your risk?

You must block any attempts by a botnet to call home. Botnets can steal your sensitive data, record users' key strokes, and become part of a larger attack on others.

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | [Patents](#)

Weblog Time: 4/17/2020 5:28:17 PM | Last Updated: 4/17/2020 5:30:24 PM

[Help](#)

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

Executive Reports

Previous Month: 3/1/2020 - 3/31/2020

Schedule Print

of a botnet that steals sensitive information. They infect your users by tricking them into clicking on links to malicious webpages or even legitimate websites that have been hacked. Or your users might become infected after downloading malicious software, browser plug-ins, or apps, or after simply viewing a compromised ad.

Advanced Threats Blocked

5,654	Browser Exploit
3,725	Phishing
1,802	Cross-site Scripting

We detected and blocked 5654 instances of browser exploit that could have infected your users.

We didn't detect any attempts by botnets to "call home."

Without Zscaler, we find that an organization can have 8-10% of its PCs infected with botnets. Companies must operate under the assumption that you have been breached but you just haven't detected it yet. Now the question becomes, how can you minimize your risk?

You must block any attempts by a botnet to call home. Botnets can steal your sensitive data, record users' key strokes, and become part of a larger attack on others.

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | [Patents](#)

Weblog Time: 4/17/2020 5:28:17 PM | Last Updated: 4/17/2020 5:30:24 PM

Help

Slide notes

Slide 43 - Slide 43

Executive Reports

Previous Month: 3/1/2020 - 3/31/2020

Schedule Print

Links to malicious websites or even legitimate websites that have been hacked. Our users might become infected after downloading malicious software, browser plug-ins, or apps, or after simply viewing a compromised ad.

Advanced Threats Blocked

Type	Count
Browser Exploit	5,654
Phishing	3,725
Cross-site Scripting	1,802

We detected and blocked 5654 instances of browser exploit that could have infected your users.

We didn't detect any attempts by botnets to "call home."

Without Zscaler, we find that an organization can have 8-10% of its PCs infected with botnets. Companies must operate under the assumption that you have been breached but you just haven't detected it yet. Now the question becomes, how can you minimize your risk?

You must block any attempts by a botnet to call home. Botnets can steal your sensitive data, record users' key strokes, and become part of a larger attack on others.

Sandbox Help

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents

Weblog Time: 4/17/2020 5:28:17 PM | Last Updated: 4/17/2020 5:30:24 PM

Slide notes

Slide 44 - Slide 44

The screenshot shows the Zscaler Dashboard interface. On the left is a vertical sidebar with icons for Executive Reports, Dashboard, Analytics (which is selected), Policy, Administration, Activation, and Search. The main content area has a header "Executive Reports" and a date range "Previous Month: 3/1/2020 - 3/31/2020". A note at the top right says "record users' key strokes, and become part of a larger attack on others." Below this is a large orange box containing the message "We found 107 new suspicious files and sent them for Sandbox." and "Zscaler has blocked 35,738 malicious files based on cloud-wide Sandbox." To the right of this box is a white "Sandbox" card with a green checkmark icon. Further down, a grey box states "Viruses represent only 55.22% of your blocked threats today" and provides a detailed explanation of modern threat evasion techniques. At the bottom right is a blue "Help" button. The footer contains copyright information "Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents" and a timestamp "Weblog Time: 4/17/2020 5:28:17 PM | Last Updated: 4/17/2020 5:30:24 PM".

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 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

Executive Reports

Previous Month: 3/1/2020 - 3/31/2020

Schedule Print

record users' key strokes, and become part of a larger attack on others.

We found 107 new suspicious files and sent them for Sandbox.

Zscaler has blocked 35,738 malicious files based on cloud-wide Sandbox.

Sandbox

✓

Viruses represent only 55.22% of your blocked threats today

Many companies have invested heavily in traditional security technologies like anti-virus protection. However, these tools are often signature-based and can't capture all of today's evolving threats. Criminals take advantage of new trends to put out malicious content, or they hijack legitimate content — for instance, a Facebook "Like" button or a common plug-in — to get your users to click and infect their own devices.

The ability to block security threats as they occur has never been more critical

As threats have grown in volume and complexity, every minute counts in response time. You must do more than detect threats. You must block them before they can cause damage. Since Zscaler sits

Help

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | [Patents](#)

Weblog Time: 4/17/2020 5:28:17 PM | Last Updated: 4/17/2020 5:30:24 PM

Slide notes

Slide 46 - Slide 46

The screenshot shows the Zscaler Dashboard interface. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area has a header "Executive Reports" and a date range "Previous Month: 3/1/2020 - 3/31/2020". At the top right are "Schedule" and "Print" buttons. A large orange banner in the center displays the message: "We found 107 new suspicious files and sent them for Sandbox." Below this, it says "Zscaler has blocked 35,738 malicious files based on cloud-wide Sandbox." To the right of the banner is a white box with a green checkmark and the word "Sandbox". The main content area below the banner contains a section titled "Viruses represent only 55.22% of your blocked threats today". It discusses the limitations of traditional security tools like anti-virus protection and the evolution of threats. A gray box below this section contains the text: "The ability to block security threats as they occur has never been more critical". It explains that threats have grown in volume and complexity, requiring real-time detection and blocking. A "Help" button is located at the bottom right of this gray box. The footer of the page includes copyright information ("Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents") and a timestamp ("Weblog Time: 4/17/2020 5:28:17 PM | Last Updated: 4/17/2020 5:30:24 PM").

Slide notes

Slide 47 - Slide 47

The screenshot shows the Zscaler Dashboard interface. On the left is a vertical sidebar with icons for Executive Reports, Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area has a header "Executive Reports" and a date range "Previous Month: 3/1/2020 - 3/31/2020". It features a large text box stating "The ability to block security threats as they occur has never been more critical" with a note about threats growing in volume and complexity. Below this is a chart titled "Security Threats as a Percentage of Overall Transactions" comparing "On your network" (0.19%) and "Cloud Averages" (0.11%). A prominent orange section below contains a "Warning: Possible infections found" message, advising users to investigate and remediate possible infections, particularly at "Headquarters". At the bottom, there's a "Compliance: Risk reduction and the threat within" section and a "Help" button. The footer includes copyright information and a timestamp.

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | [Patents](#)

Weblog Time: 4/17/2020 5:28:17 PM | Last Updated: 4/17/2020 5:30:24 PM

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

The screenshot shows the Zscaler Dashboard interface. On the left is a vertical sidebar with icons for Executive Reports, Dashboard, Analytics, Policy, Administration, Activation, Search, and Help. The main content area has a header "Executive Reports" and a date range "Previous Month: 3/1/2020 - 3/31/2020". It features a large text box stating "The ability to block security threats as they occur has never been more critical" with a note about threats growing in volume and complexity. Below this is a chart titled "Security Threats as a Percentage of Overall Transactions" comparing "On your network" (0.19%) to "Cloud Averages" (0.11%). A prominent orange section below contains a warning about possible infections found at "Head Quarters". At the bottom, there's a "Compliance: Risk reduction and the threat within" section with a note about employees being a threat.

The dashboard displays the following key information:

- Security Threats as a Percentage of Overall Transactions:**
 - On your network: 0.19%
 - Cloud Averages: 0.11%
- Warning: Possible infections found**

We recommend investigating and remediating the possible infections noted below. You should re-image infected devices immediately.
- Top Locations with Possible Infections:**
 - 60.310 Head Quarters
- Compliance: Risk reduction and the threat within**

Your employees may also present a threat to the organization, whether unintentional or malicious.

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | [Patents](#)

Weblog Time: 4/17/2020 5:28:17 PM | Last Updated: 4/17/2020 5:30:24 PM

Slide notes

Slide 49 - Slide 49

The screenshot shows the Zscaler Dashboard interface. On the left, a vertical sidebar lists navigation options: Executive Reports, Dashboard (selected), Analytics, Policy, Administration, Activation, Search, and Help. The main content area has a header "Executive Reports" and a date range "Previous Month: 3/1/2020 - 3/31/2020". It features a large text block: "occur has never been more critical" followed by a paragraph about threats growing in volume and complexity. Below this is a chart titled "Security Threats as a Percentage of Overall Transactions" comparing "On your network" (0.19%) and "Cloud Averages" (0.11%). A prominent orange section below the chart displays a "Warning: Possible infections found" message, advising users to investigate and remediate possible infections, particularly at "Headquarters". At the bottom, a "Compliance: Risk reduction and the threat within" section discusses employee threats. The footer includes copyright information ("Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents"), a timestamp ("Weblog Time: 4/17/2020 5:28:17 PM | Last Updated: 4/17/2020 5:30:24 PM"), and a Help button.

Slide notes

Slide 50 - Slide 50

The screenshot shows the 'Executive Reports' dashboard. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Policy, Administration, Activation, Search, and Help. The main content area features a large orange header bar. Below it, a central panel displays the 'Compliance: Risk reduction and the threat within' section. It includes a message: 'Your employees may also present a threat to the organization, whether unintentional or malicious.' A chart titled 'Your URL Classes Blocked / Allowed' shows the following data:

Category	Blocked	Allowed
Business Use	2.7 M	34.6 M
Bandwidth Loss	1 M	14 M
Productivity Loss	1 M	2.4 M
General Surfing	2.9 K	867.4 K
Legal Liability	412.7 K	0
Adv. Security Risk	11.2 K	0
Privacy Risk	0	379

A legend at the bottom indicates that red bars represent 'Blocked' and grey bars represent 'Allowed'. To the right, two smaller boxes show 'Top Categories for Liability Exposure Allowed' (empty) and 'Top Categories for Liability Exposure Blocked' (listing Nudity, Gambling, Copyright Infringement, and Lingerie/Bikini). The bottom of the screen includes copyright information, a help icon, and a timestamp.

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

The screenshot shows the 'Executive Reports' section of the dashboard. The left sidebar includes icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area displays a red header bar with the title 'Compliance: Risk reduction and the threat within'. Below it, a message states: 'Your employees may also present a threat to the organization, whether unintentional or malicious.' A chart titled 'Your URL Classes Blocked / Allowed' lists categories and their counts:

Category	Blocked	Allowed
Business Use	2.7 M	34.6 M
Bandwidth Loss	1	14 M
Productivity Loss	1	2.4 M
General Surfing	2.9 K	867.4 K
Legal Liability	412.7 K	0
Adv. Security Risk	11.2 K	0
Privacy Risk	0	379

A legend indicates that red bars represent 'Blocked' and grey bars represent 'Allowed'. Two smaller charts show 'Top Categories for Liability Exposure Allowed' (no violations) and 'Top Categories for Liability Exposure Blocked' (with counts: Nudity 103,383, Gambling 103,377, Copyright Infringement 103,027, Lingerie/Bikini 102,953).

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | [Patents](#)

Weblog Time: 4/17/2020 5:28:17 PM | Last Updated: 4/17/2020 5:30:24 PM

[Help](#)

Slide notes

Slide 52 - Slide 52

The screenshot shows the Zscaler Dashboard interface. On the left, a vertical sidebar lists navigation options: Executive Reports, Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area displays a report titled "Compliance: Risk reduction and the threat within". A sub-section titled "Your URL Classes Blocked / Allowed" provides a breakdown of blocked vs allowed traffic across various categories. Below this are four smaller cards: "Top Categories for Liability Exposure Allowed" (no violations), "Top Categories for Liability Exposure Blocked" (listing Nudity, Gambling, Copyright Infringement, and Lingerie/Bikini), "Top Locations for Liability Exposure" (Head Quarters), and "Top Departments for Liability Exposure" (Support). The bottom of the screen includes copyright information, a help icon, and a timestamp.

Executive Reports

Previous Month: 3/1/2020 - 3/31/2020

Schedule Print

Compliance: Risk reduction and the threat within

Your employees may also present a threat to the organization, whether unintentional or malicious.

Your URL Classes Blocked / Allowed

Business Use: Blocked 2.7 M / Allowed 34.6 M
Bandwidth Loss: Blocked 1 / Allowed 14 M
Productivity Loss: Blocked 1 / Allowed 2.4 M
General Surfing: Blocked 2.9 K / Allowed 867.4 K
Legal Liability: Blocked 412.7 K / Allowed 0
Adv. Security Risk: Blocked 11.2 K / Allowed 0
Privacy Risk: Blocked 0 / Allowed 379

Blocked Allowed

Top Categories for Liability Exposure Allowed

Your employees did not have any policy violations during this time period.

Top Categories for Liability Exposure Blocked

103,383 Nudity
103,377 Gambling
103,027 Copyright Infringement
102,953 Lingerie/Bikini

Top Locations for Liability Exposure

412,740 Head Quarters

Top Departments for Liability Exposure

77,682 Support

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | [Patents](#)

Weblog Time: 4/17/2020 5:28:17 PM | Last Updated: 4/17/2020 5:30:24 PM

Help

Slide notes

Slide 53 - Slide 53

The screenshot displays the 'Executive Reports' section of the dashboard. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area shows four report cards:

- Top Categories for Liability Exposure Allowed:** Your employees did not have any policy violations during this time period.
- Top Categories for Liability Exposure Blocked:**

103,383	Nudity
103,377	Gambling
103,027	Copyright Infringement
102,953	Lingerie/Bikini
- Top Locations for Liability Exposure:** 412,740 Head Quarters
- Top Departments for Liability Exposure:**

77,682	Support
48,180	Sales Engineering
46,667	Sales
41,208	Research & Development
36,907	Engineering Development

A central chart compares policy violation percentages: **5.50%** (On your network) and **6.01%** (Cloud Averages).

At the bottom, a callout states: **Productivity: Gain visibility into how your resources are being used**. The footer includes copyright information, a help icon, and system status: Weblog Time: 4/17/2020 5:28:17 PM | Last Updated: 4/17/2020 5:30:24 PM.

Slide notes

Slide 54 - Slide 54

The screenshot shows the 'Executive Reports' section of the dashboard. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, Search, and Help. The main area displays four donut charts under the heading 'Productivity: Gain visibility into how your resources are being used'.

1. **Webmail by transactions:** Total 409.4 K. Legend: Outlook (Personal) (blue), Outlook (green), GMail (yellow).
2. **Development Apps by transactions:** Total 677.5 K. Legend: Github (blue), Microsoft Codeplex (green), Microsoft Visual Studio (yellow), Cloudant (red), Bugaware (light green).
3. **Streaming Media by bytes:** A small chart showing a very low volume.
4. **Collaboration Apps by transactions:** A small chart showing a very low volume.

At the bottom, there are copyright information (Copyright 2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents) and a timestamp (Weblog Time: 4/17/2020 5:28:17 PM | Last Updated: 4/17/2020 5:30:24 PM).

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

Executive Reports

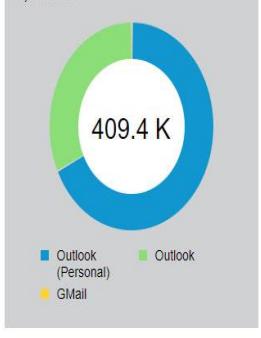
Previous Month: 3/1/2020 - 3/31/2020

Schedule Print

Productivity: Gain visibility into how your resources are being used

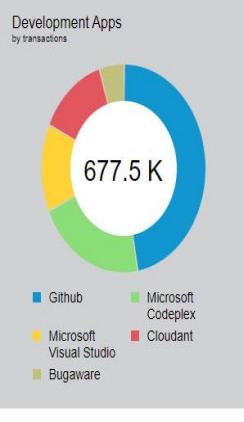
You can't turn off the Internet. The Internet has become a key business enabler. Yet the challenge of ensuring secure access is only growing. We can help by providing you with visibility into what users are doing so that you can make data-driven decisions. Instead of limiting what your users do, give them the tools they need to get the job done.

Webmail by transactions



Category	Value
Outlook (Personal)	409.4 K
Outlook	~10 K
GMail	~10 K

Development Apps by transactions



Category	Value
Github	677.5 K
Microsoft Codeplex	~10 K
Microsoft Visual Studio	~10 K
Cloudant	~10 K
Bugaware	~10 K

Streaming Media by bytes



Category	Value
Unknown	~10 K
Unknown	~10 K

Collaboration Apps by transactions



Category	Value
Unknown	~10 K
Unknown	~10 K

Help

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents

Weblog Time: 4/17/2020 5:28:17 PM | Last Updated: 4/17/2020 5:30:24 PM

Slide notes

Slide 56 - Slide 56

Executive Reports

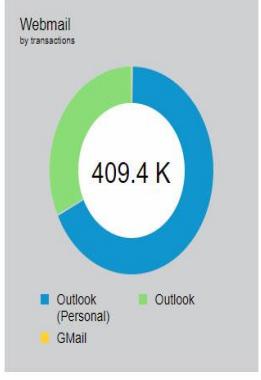
Previous Month: 3/1/2020 - 3/31/2020

Schedule Print

Productivity: Gain visibility into how your resources are being used

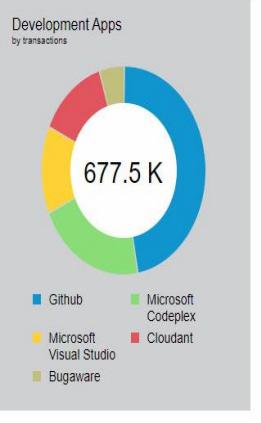
You can't turn off the Internet. The Internet has become a key business enabler. Yet the challenge of ensuring secure access is only growing. We can help by providing you with visibility into what users are doing so that you can make data-driven decisions. Instead of limiting what your users do, give them the tools they need to get the job done.

Webmail by transactions



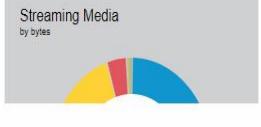
Category	Value
Outlook (Personal)	409.4 K
Outlook	~10%
GMail	~10%

Development Apps by transactions



Category	Value
Github	~30%
Microsoft Codeplex	~20%
Microsoft Visual Studio	~15%
Cloudant	~10%
Bugaware	~15%

Streaming Media by bytes



Category	Value
YouTube	~50%
Netflix	~30%
Hulu	~20%

Collaboration Apps



Category	Value
Google Drive	~50%
Microsoft SharePoint	~50%

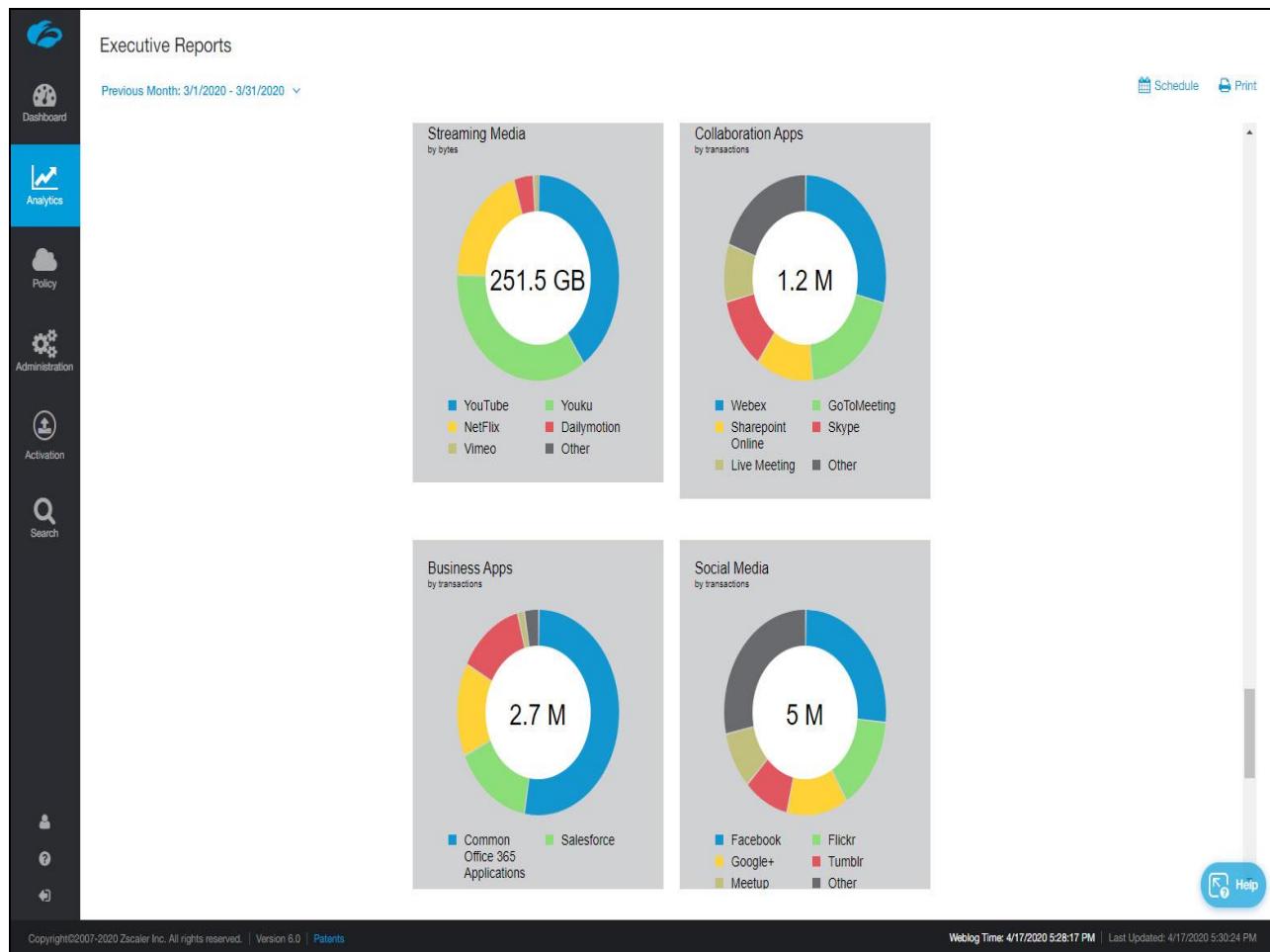
Help

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents

Weblog Time: 4/17/2020 5:28:17 PM | Last Updated: 4/17/2020 5:30:24 PM

Slide notes

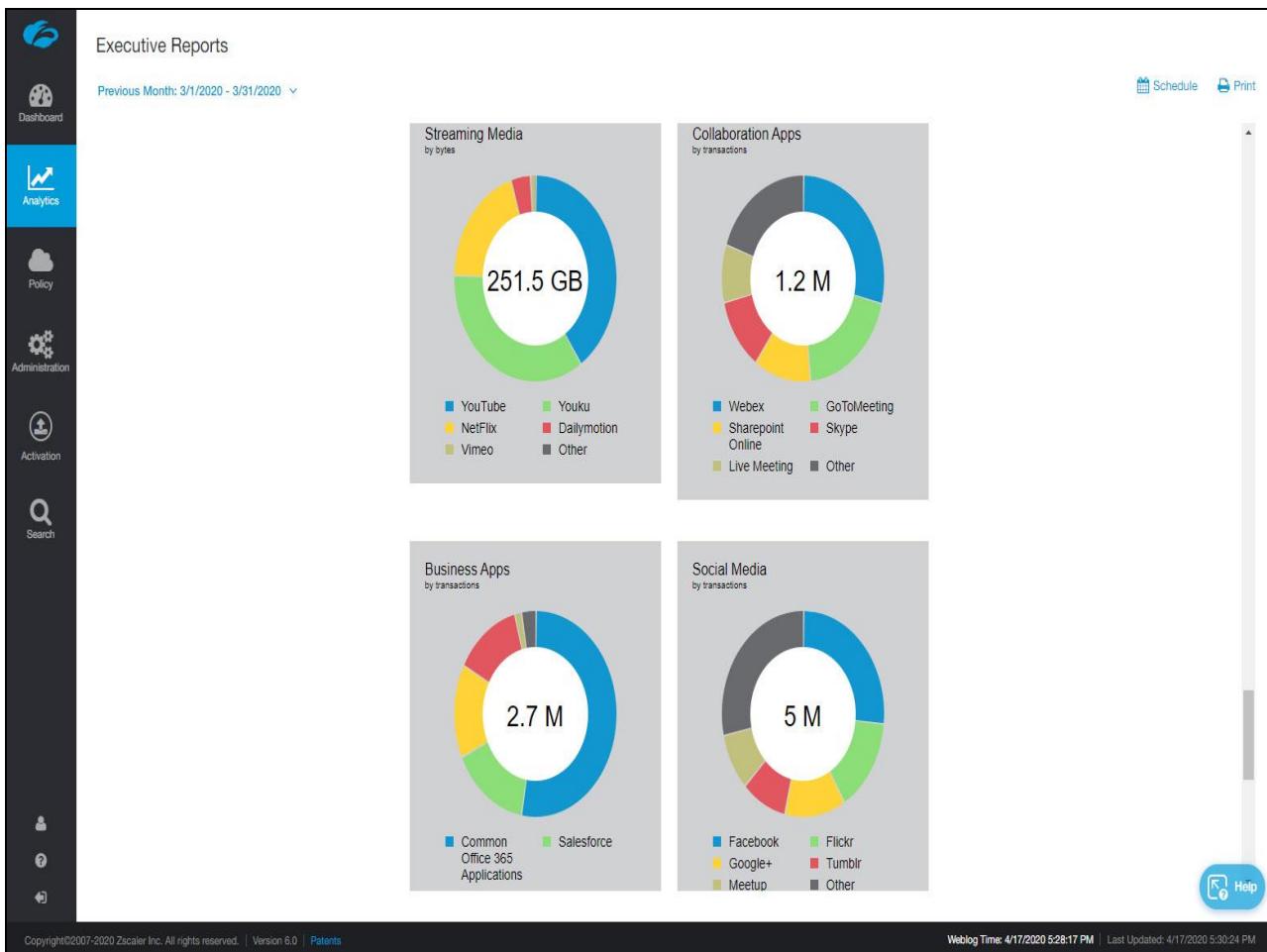
Slide 57 - Slide 57



Slide notes

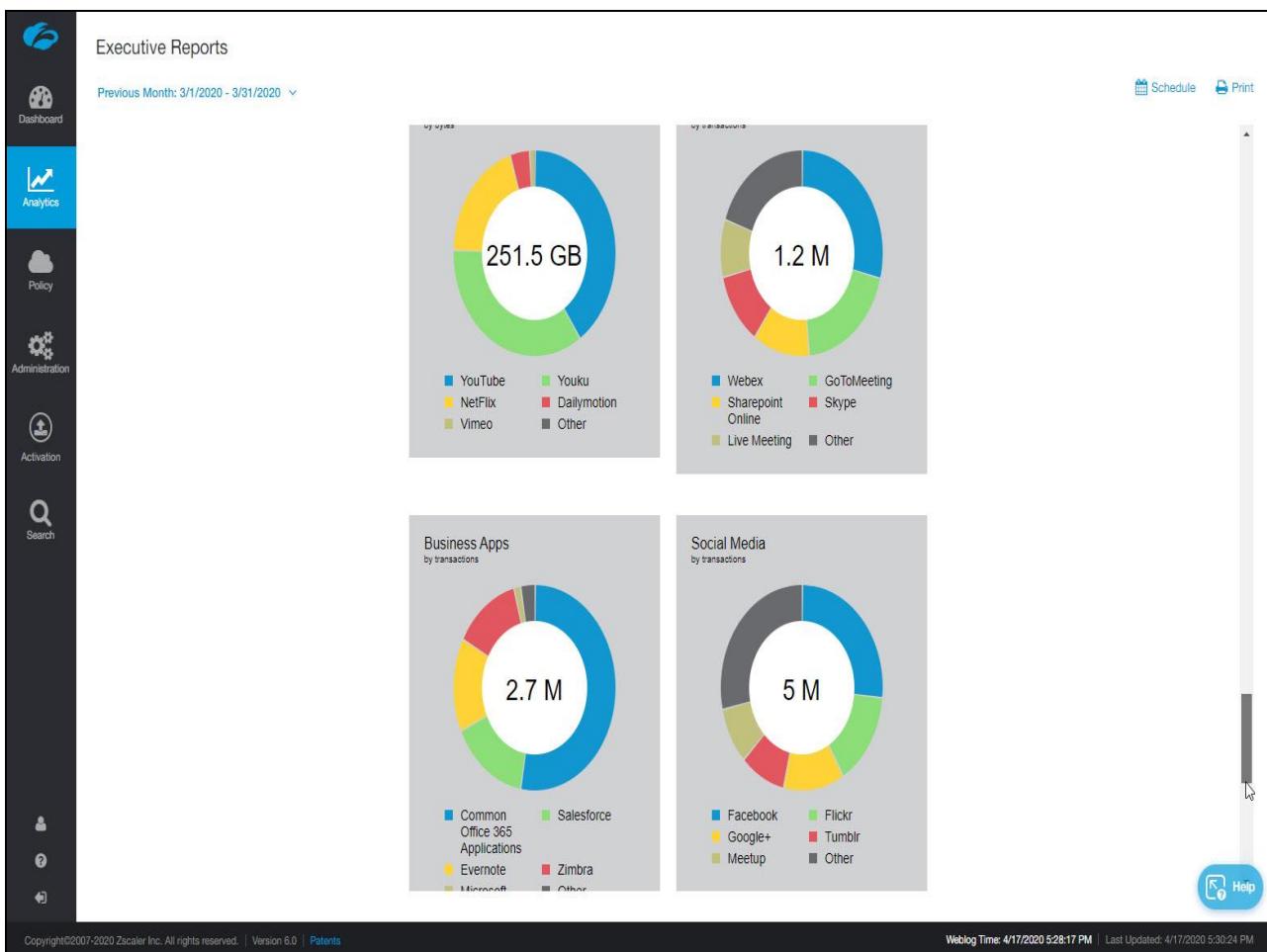
If, for example, you see users spending a lot of time on Facebook, and your organization does not have a legitimate business use for Facebook you know there is an issue that needs to be addressed.

Slide 58 - Slide 58



Slide notes

Slide 59 - Slide 59



Slide notes

Slide 60 - Slide 60

The Zscaler subscriptions you have turned on are highlighted below:

Web Security	✓ Protects against malicious URL requests
Advanced Web Security	✓ Protects against botnets, adware, spyware, cross-site scripting, and more
Cloud Sandbox	✓ Protects against zero-day threats and targeted attacks
Standard Firewall	✓ Provides powerful security with port and protocol controls
Next Generation Firewall	✓ Provides powerful security with application visibility and control
Data Loss Prevention	✓ Protects your confidential information and intellectual property
Mobile Security	✓ Protects users on mobile devices which you provide or which they own
Bandwidth Controls	✓ Provides you with control over bandwidth usage

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | [Patents](#)

Weblog Time: 4/17/2020 5:28:17 PM | Last Updated: 4/17/2020 5:30:24 PM

[Help](#)

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 -

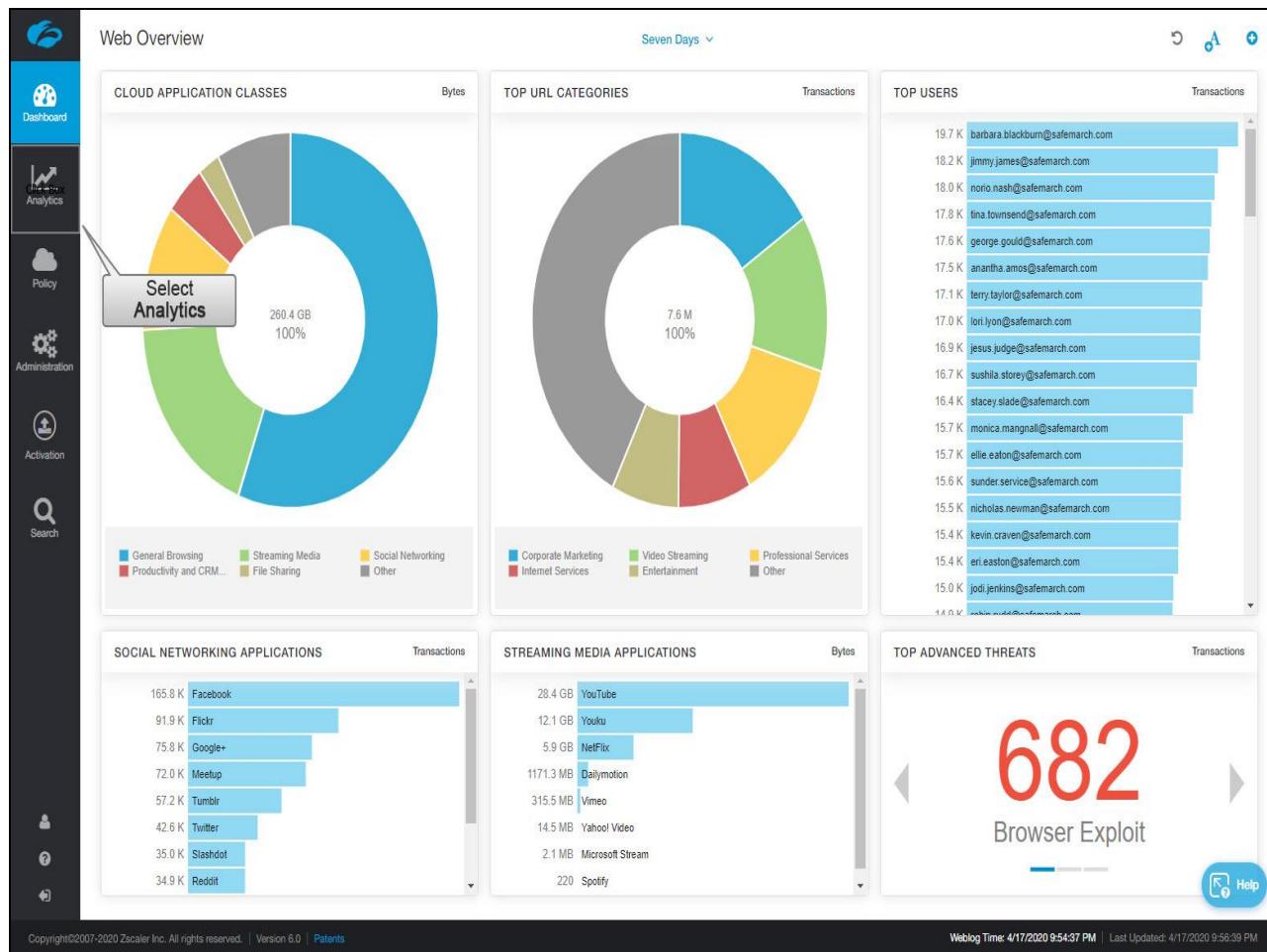
Industry Peer Comparison Report



Industry Peer Comparison Report

Slide notes

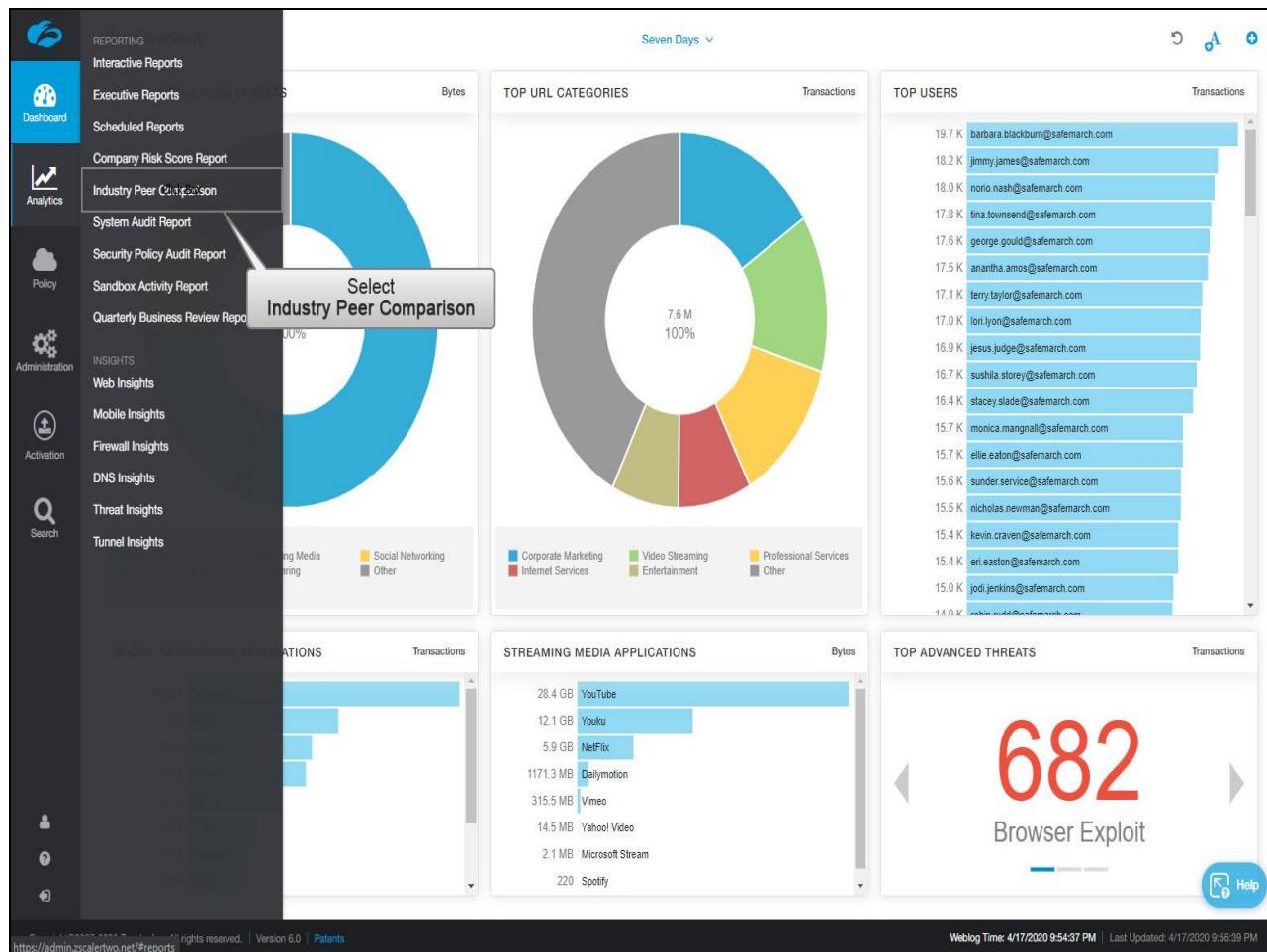
Slide 62 - Slide 62



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**.

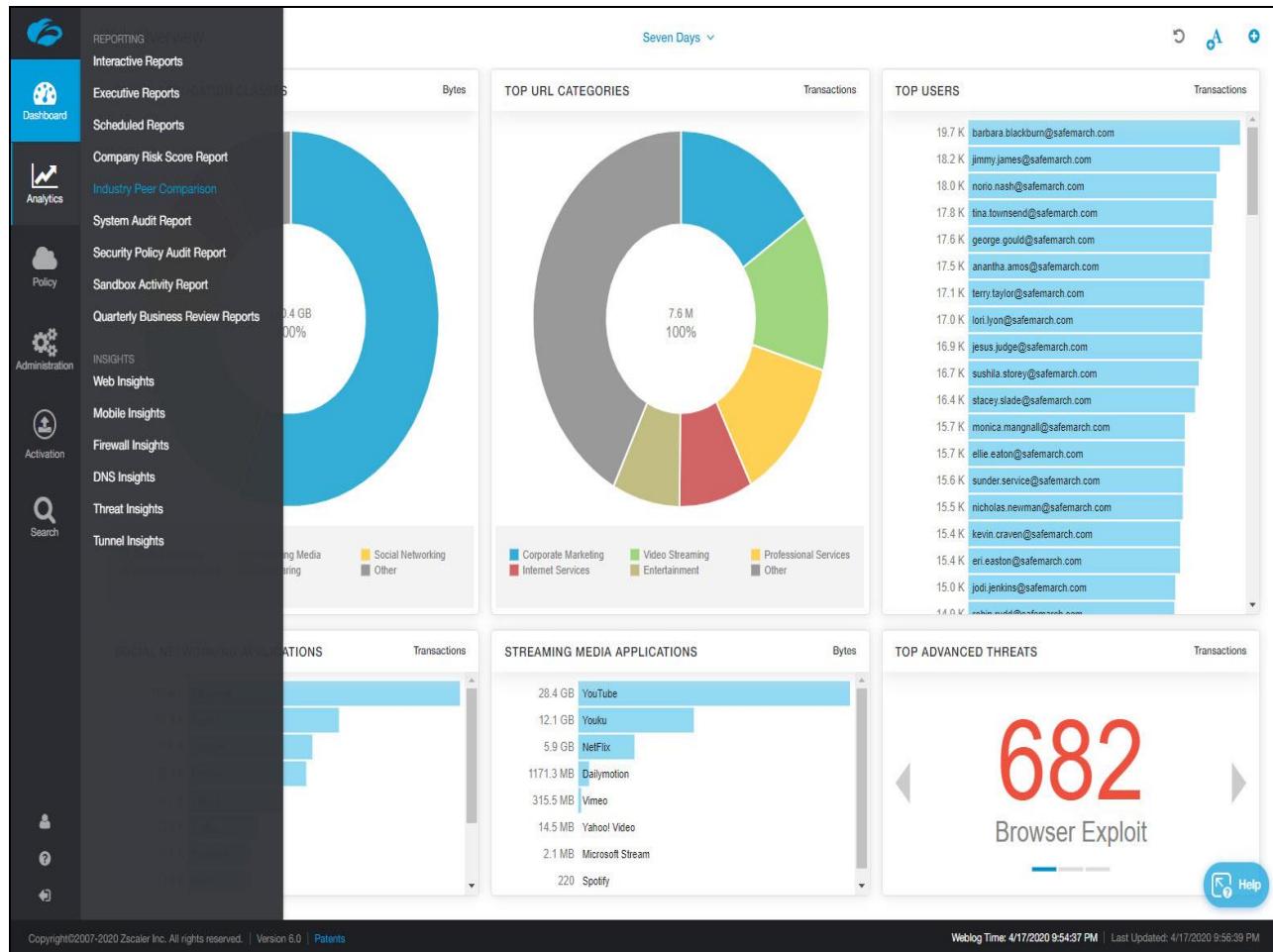
Slide 63 - Slide 63



Slide notes

Then Industry Peer Comparison.

Slide 64 - Slide 64



Slide notes

Slide 65 - Slide 65

Industry Peer Comparison Report March 2020

This report compares your organization's performance for the preceding month to that of both peer organizations and all companies using our cloud service.

YOUR	PEER AVERAGE	CLOUD AVERAGE	EXPLANATION
Overview			Total Transactions
Transactions Blocked	5.69%	4.05%	6.12%
Policy Violations	5.51%	3.94%	6.01%
Threats Blocked	0.19%	0.11%	0.10%

Threats by Category Total Threats

- Malware Detection: 55.0%
- Advanced Threats: 34.3%
- Cloud Sandbox: 9.7%

Recreational Total Bytes

- Social Networking: 11.88%
- 5.60%
- 3.67%

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents

Weblog Time: 4/17/2020 9:54:37 PM | Last Updated: 4/17/2020 9:56:39 PM

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 organization's 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

Industry Peer Comparison Report

This report compares your organization's performance against that of both peer organizations and all companies using our cloud service.

YOUR COMPANY

- Business Vertical: Technology & Communication
- Geographic Region: North America
- Business Size: 1-2000

March 2020

	PEER AVERAGE	CLOUD AVERAGE	EXPLANATION
Overview			Total Transactions
Transactions Blocked	5.69%	4.05%	6.12%
Policy Violations	5.51%	3.94%	6.01%
Threats Blocked	0.19%	0.11%	0.10%

Threats by Category

Total Threats

We identify advanced threats using streaming pattern matches, AV signatures, file hash match, and other threat indicators. Our multi-tenant cloud then shares threat information across millions of users. Any threat identified in our cloud is, within seconds, blocked for all customers.

Recreational

Total Bytes

Recreational includes applications categorized under the Social Networking and Blogging

Help

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents

Weblog Time: 4/17/2020 9:54:37 PM | Last Updated: 4/17/2020 9:56:39 PM

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

Industry Peer Comparison Report i

March 2020

This report compares your organization's performance for the preceding month to that of both peer organizations and all companies using our cloud service.

	YOUR AVERAGE	PEER AVERAGE	CLOUD AVERAGE	EXPLANATION
Overview				i Total Transactions
Transactions Blocked	5.69%	4.05%	6.12%	
Policy Violations	5.51%	3.94%	6.01%	i Our cloud service processes more than 40 Billion transactions, blocks more than 100 Million threats and performs more than 120 thousand security updates every day.
Threats Blocked	0.19%	0.11%	0.10%	
Threats by Category				i Total Threats
Malware Detection	34.3%	55.0%	5.6%	
Advanced Threats	10.7%	9.7%	0.6%	
Cloud Sandbox	55.0%	93.7%	3.1%	We identify advanced threats using streaming pattern matches, AV signatures, file hash match, and other threat indicators. Our multi-tenant cloud then shares threat information across millions of users. Any threat identified in our cloud is, within seconds, blocked for all customers.
Recreational				i Total Bytes
Social Networking	11.88%	5.60%	3.67%	Recreational includes applications categorized under the Social Networking and Blogging

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | [Patents](#)

Weblog Time: 4/17/2020 9:54:37 PM | Last Updated: 4/17/2020 9:56:39 PM

i Help

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

Industry Peer Comparison Report (i)

March 2020

This report compares your organization's performance for the preceding month to that of both peer organizations and all companies using our cloud service.

	YOUR AVERAGE	PEER AVERAGE	CLOUD AVERAGE	EXPLANATION
Overview				<small>Total Transactions</small>
Transactions Blocked	5.69%	4.05%	6.12%	<small>Our cloud service processes more than 40 Billion transactions, blocks more than 100 Million threats and performs more than 120 thousand security updates every day.</small>
Policy Violations	5.51%	3.94%	6.01%	
Threats Blocked	0.19%	0.11%	0.10%	
Threats by Category				<small>Total Threats</small>
Malware Detection				<small>We identify advanced threats using streaming pattern matches, AV signatures, file hash match, and other threat indicators. Our multi-tenant cloud then shares threat information across millions of users. Any threat identified in our cloud is, within seconds, blocked for all customers.</small>
Recreational				<small>Total Bytes</small>
Social Networking				<small>Recreational includes applications categorized under the Social Networking and Blogging categories as well as Streaming Media categories.</small>

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | [Patents](#)

Weblog Time: 4/17/2020 9:54:37 PM | Last Updated: 4/17/2020 9:56:39 PM

[Help](#)

Slide notes

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

Slide 69 - Slide 69

Industry Peer Comparison Report  March 2020

This report compares your organization's performance for the preceding month to that of both peer organizations and all companies using our cloud service.

	YOUR AVERAGE	PEER AVERAGE	CLOUD AVERAGE	EXPLANATION
Threats by Category				
Malware Detection	34.3%	55.0%	0.7%	5.6%
Advanced Threats	10.7%	93.7%	96.4%	3.1%
Cloud Sandbox				
Recreational				
Social Networking	11.88%	5.60%	3.67%	Total Bytes
Video Streaming	12.80%	9.17%	10.53%	Total Bytes
Productivity Applications				
Office 365	3.47%	15.83%	23.66%	Total Bytes
Other Productivity Applications	4.68%	1.52%	0.39%	Total Bytes

 Help

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | [Patents](#)

Weblog Time: 4/17/2020 9:54:37 PM | Last Updated: 4/17/2020 9:56:39 PM

Slide notes

Slide 70 - Slide 70

Industry Peer Comparison Report i

March 2020

This report compares your organization's performance for the preceding month to that of both peer organizations and all companies using our cloud service.

	YOUR AVERAGE	PEER AVERAGE	CLOUD AVERAGE	EXPLANATION
Threats by Category				
Malware Detection	34.3%	55.0%	5.6%	We identify advanced threats using streaming pattern matches, AV signatures, file hash match, and other threat indicators. Our multi-tenant cloud then shares threat information across millions of users. Any threat identified in our cloud is, within seconds, blocked for all customers.
Advanced Threats	10.7%	9.7%	3.1%	
Cloud Sandbox		93.7%	96.4%	
Recreational				
Social Networking	11.88%	5.60%	3.67%	Recreational includes applications categorized under the Social Networking and Blogging category as well as Streaming Media category. These categories include applications like Facebook, WordPress, Dropbox and YouTube.
Video Streaming	12.80%	9.17%	10.53%	
Productivity Applications				
Office 365	3.47%	15.83%	23.66%	Our cloud service increases your productivity by providing faster access to your Office 365 applications. A dedicated dashboard provides real-time visibility into your organization's Office 365 traffic.
Other Productivity Applications	4.68%	1.52%	0.39%	

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | [Patents](#)

Weblog Time: 4/17/2020 9:54:37 PM | Last Updated: 4/17/2020 9:56:39 PM

i Total Threats Total Bytes Total Bytes Help

Slide notes

Slide 71 - Slide 71

Industry Peer Comparison Report i

March 2020

This report compares your organization's performance for the preceding month to that of both peer organizations and all companies using our cloud service.

	YOUR AVERAGE	PEER AVERAGE	CLOUD AVERAGE	EXPLANATION
Overview				
Transactions Blocked	5.69%	4.05%	6.12%	
Policy Violations	5.51%	3.94%	6.01%	Total Transactions Our cloud service processes more than 40 Billion transactions, blocks more than 100 Million threats and performs more than 120 thousand security updates every day.
Threats Blocked	0.19%	0.11%	0.10%	
Threats by Category				
Malware Detection				Total Threats We identify advanced threats using streaming pattern matches, AV signatures, file hash match, and other threat indicators. Our multi-tenant cloud then shares threat information across millions of users. Any threat identified in our cloud is, within seconds, blocked for all customers.
Recreational				
Social Networking				Total Bytes Recreational includes applications categorized under the Social Networking and Blogging

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | [Patents](#)

Weblog Time: 4/17/2020 9:54:37 PM | Last Updated: 4/17/2020 9:56:39 PM

[Help](#)

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

Industry Peer Comparison Report ?

March 2020

This report compares your organization's performance for the preceding month to that of both peer organizations and all companies using our cloud service.

	YOUR AVERAGE	PEER AVERAGE	CLOUD AVERAGE	EXPLANATION
Overview				Total Transactions
Transactions Blocked	5.69%	4.05%	6.12%	
Policy Violations	5.51%	3.94%	6.01%	Total Threats
Threats Blocked	0.19%	0.11%	0.10%	
Threats by Category				Total Threats
Malware Detection	34.3%	55.0%	0.7%	
Advanced Threats	10.7%	5.6%	3.1%	
Cloud Sandbox	55.0%	0.6%	93.7%	Total Bytes
Recreational				Total Bytes
Social Networking	11.88%	5.60%	3.67%	Help

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | [Patents](#)

Weblog Time: 4/17/2020 9:54:37 PM | Last Updated: 4/17/2020 9:56:39 PM

Slide notes

Slide 73 - Slide 73

Industry Peer Comparison Report i

March 2020

This report compares your organization's performance for the preceding month to that of both peer organizations and all companies using our cloud service.

	YOUR AVERAGE	PEER AVERAGE	CLOUD AVERAGE	EXPLANATION
Threats Blocked	0.19%	0.11%	0.10%	threats and performs more than 120 thousand security updates every day.

Threats by Category

Total Threats

Category	Percentage
Malware Detection	34.3%
Advanced Threats	55.0%
Cloud Sandbox	10.7%

We identify advanced threats using streaming pattern matches, AV signatures, file hash match, and other threat indicators. Our multi-tenant cloud then shares threat information across millions of users. Any threat identified in our cloud is, within seconds, blocked for all customers.

Recreational

Total Bytes

Category	Percentage
Social Networking	11.88%
Video Streaming	12.80%
Productivity Applications	15.83%

Recreational includes applications categorized under the Social Networking and Blogging category as well as Streaming Media category. These categories include applications like Facebook, WordPress, Dropbox and YouTube.

Productivity Applications

Total Bytes

Category	Percentage
Social Networking	3.67%
Video Streaming	10.53%
Productivity Applications	23.66%

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | [Patents](#)

Weblog Time: 4/17/2020 9:54:37 PM | Last Updated: 4/17/2020 9:56:39 PM

Help

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

Industry Peer Comparison Report i

March 2020

This report compares your organization's performance for the preceding month to that of both peer organizations and all companies using our cloud service.

	YOUR AVERAGE	PEER AVERAGE	CLOUD AVERAGE	EXPLANATION
Threats Blocked	0.19%	0.11%	0.10%	Identifies and performs more than 120 thousand security updates every day.

Threats by Category

Total Threats

Category	Percentage
Malware Detection	34.3%
Advanced Threats	55.0%
Cloud Sandbox	10.7%

We identify advanced threats using streaming pattern matches, AV signatures, file hash match, and other threat indicators. Our multi-tenant cloud then shares threat information across millions of users. Any threat identified in our cloud is, within seconds, blocked for all customers.

Recreational

Total Bytes

Category	Percentage
Social Networking	11.88%
Video Streaming	12.80%
Productivity Applications	5.60%

Recreational includes applications categorized under the Social Networking and Blogging category as well as Streaming Media category. These categories include applications like Facebook, WordPress, Dropbox and YouTube.

Productivity Applications

Total Bytes

Category	Percentage
Office 365	23.66%

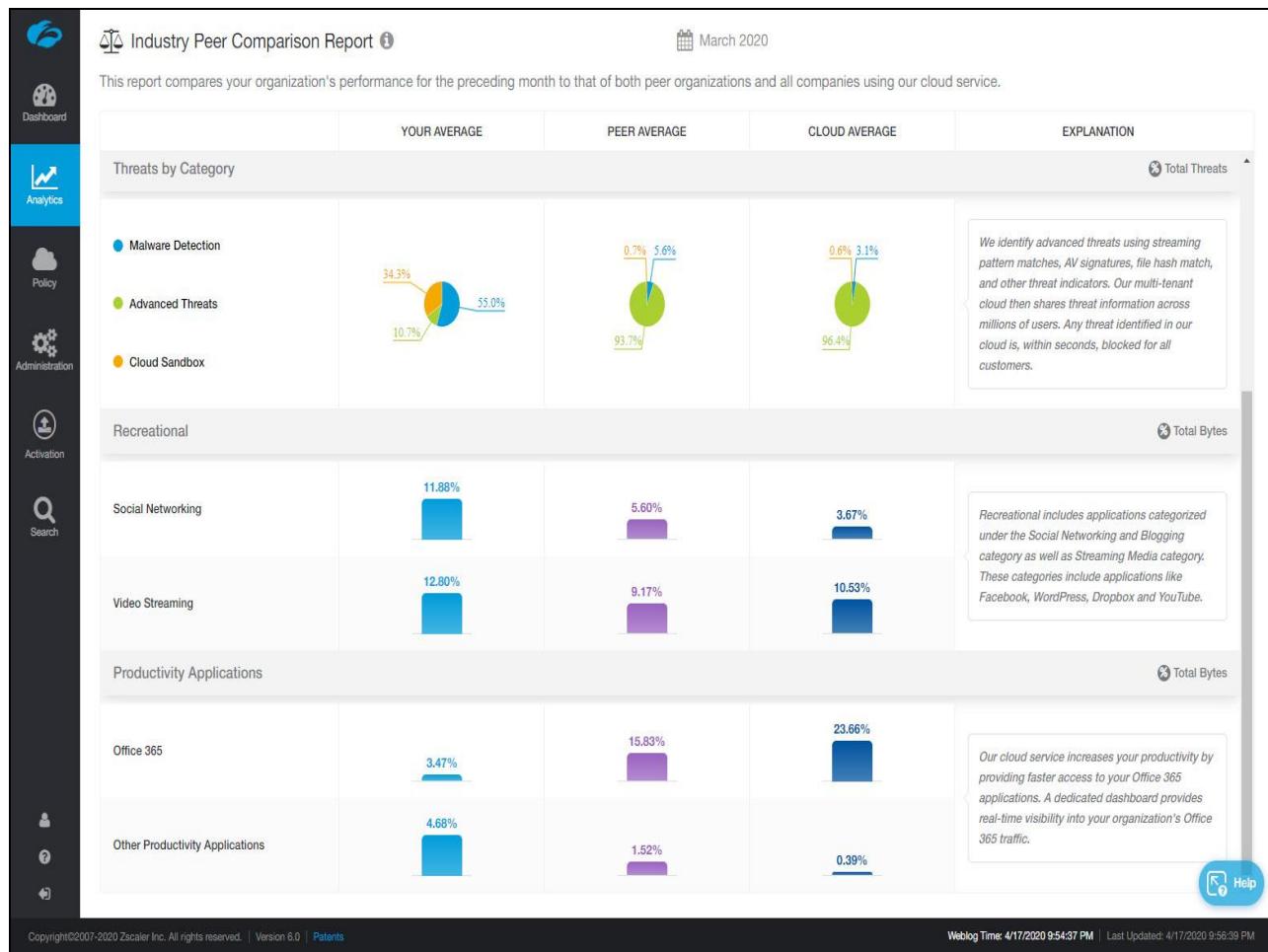
Help

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | [Patents](#)

Weblog Time: 4/17/2020 9:54:37 PM | Last Updated: 4/17/2020 9:56:39 PM

Slide notes

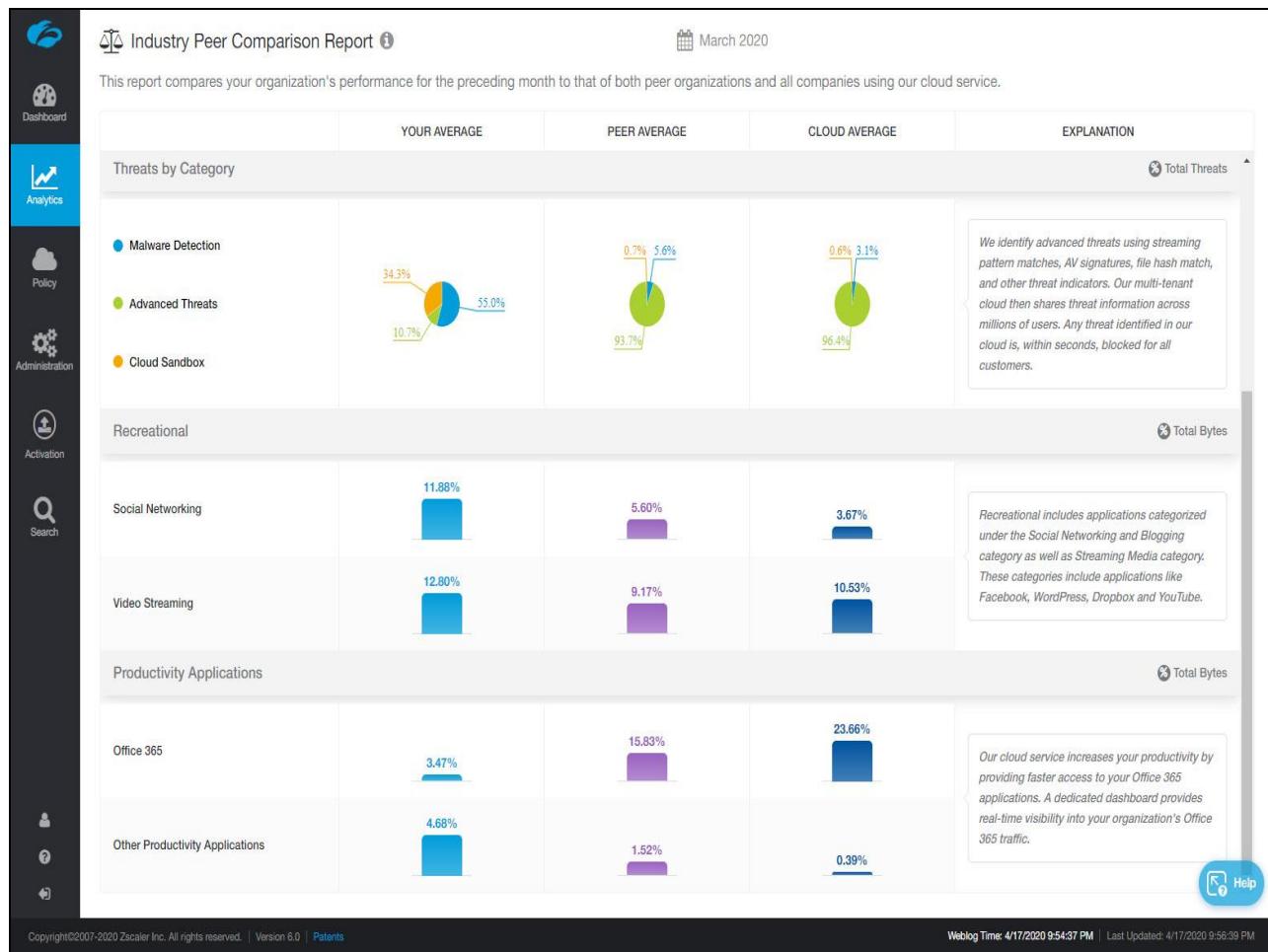
Slide 75 - Slide 75



Slide notes

Moving down to “Recreational” we see that our employees are spending more time using social networking applications and video streaming applications than 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

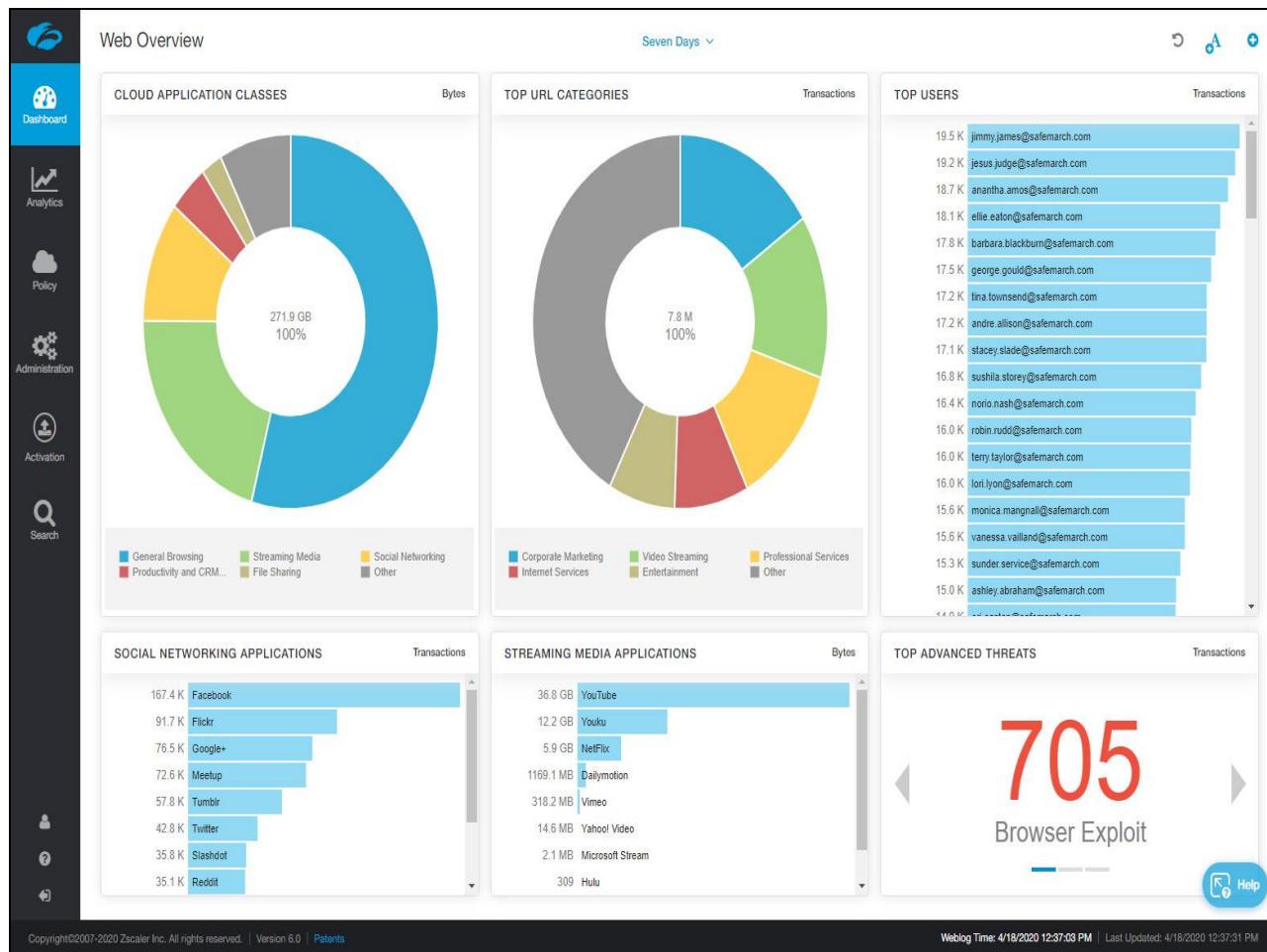


Problem tracking using the Dashboard and Reporting

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.

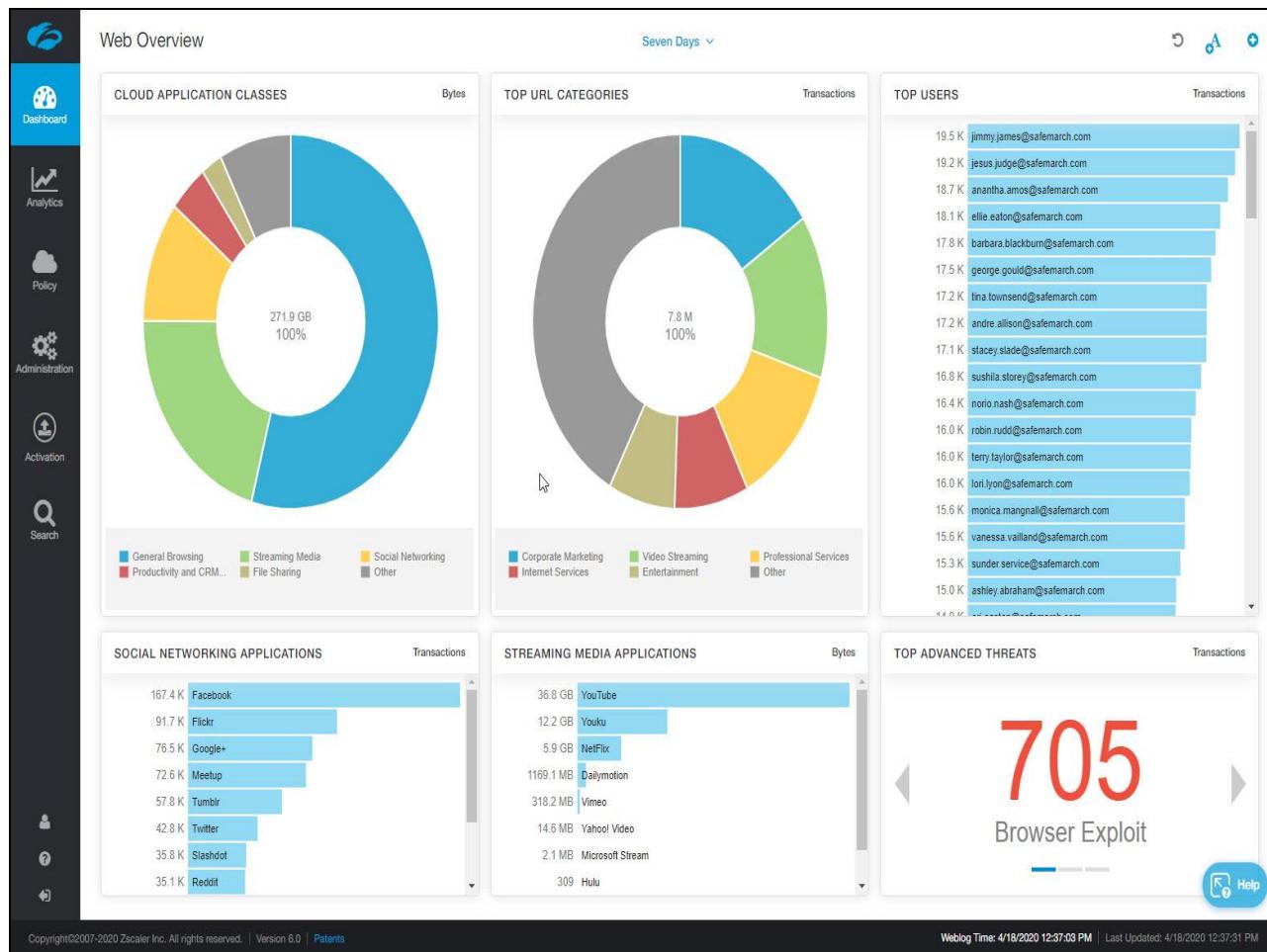
Slide 78 - Slide 78



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 of URL categories or Cloud applications, for example, is flowing through your network.

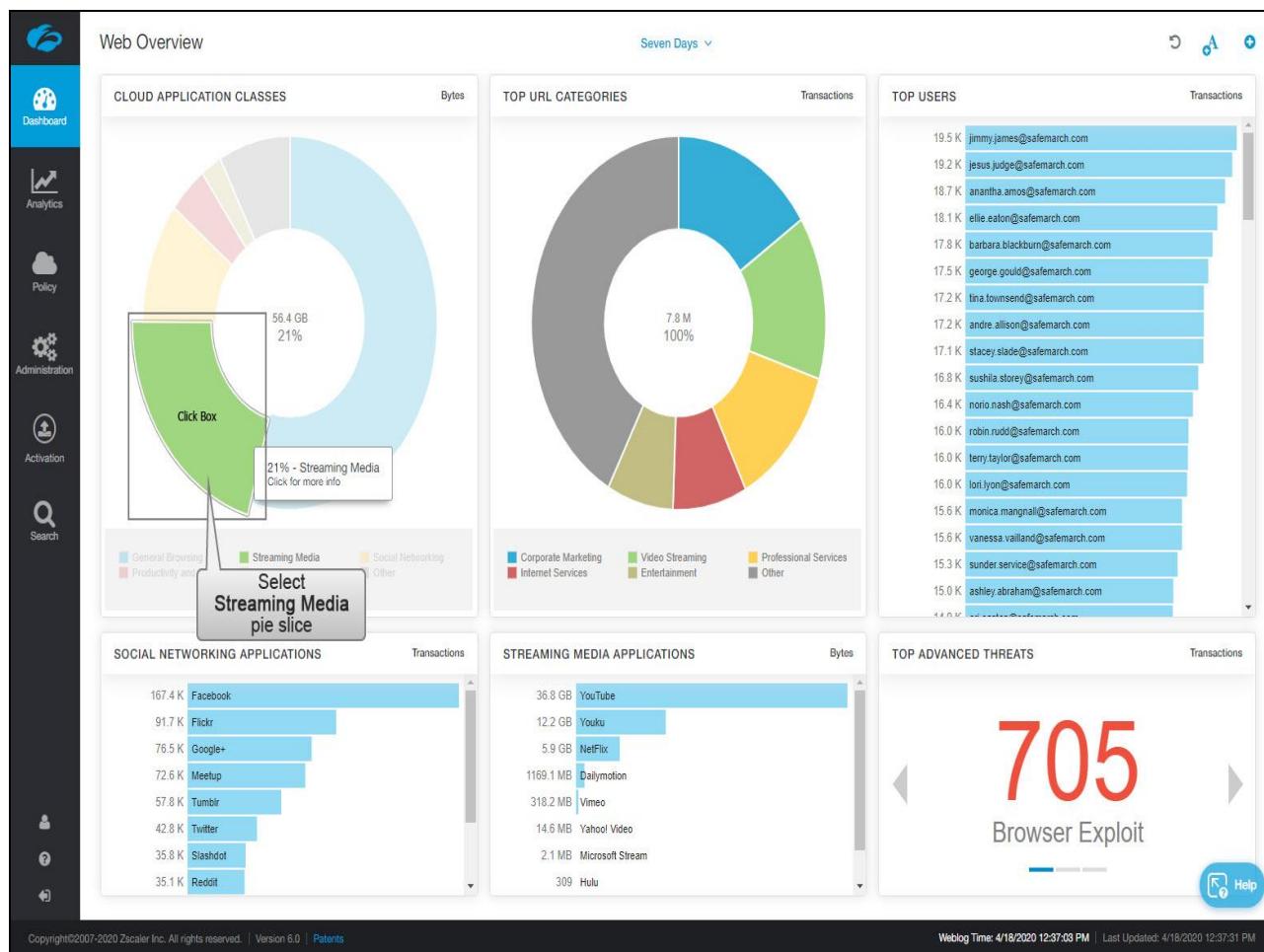
Slide 79 - Slide 79



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.

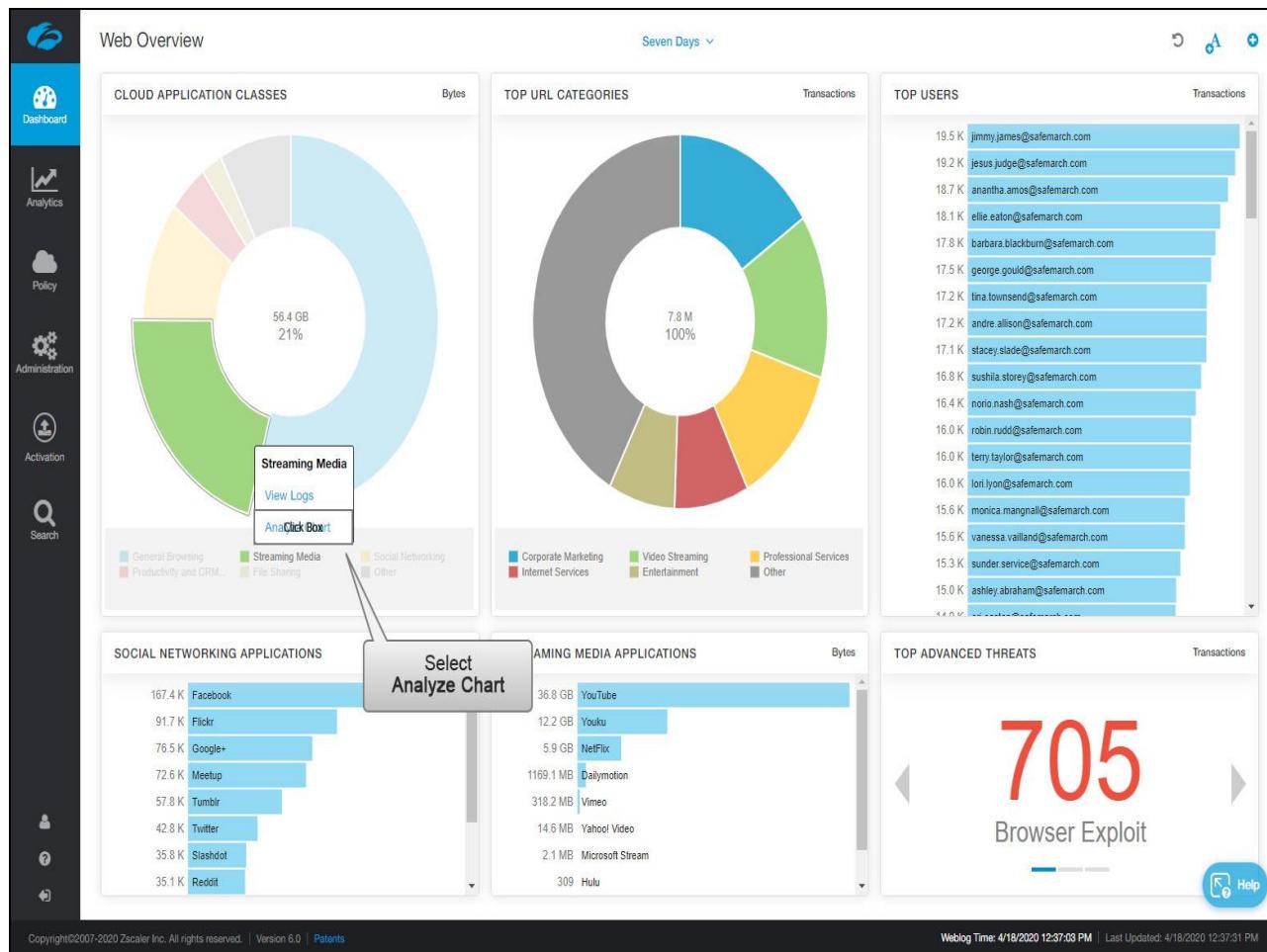
Slide 80 - Slide 80



Slide notes

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

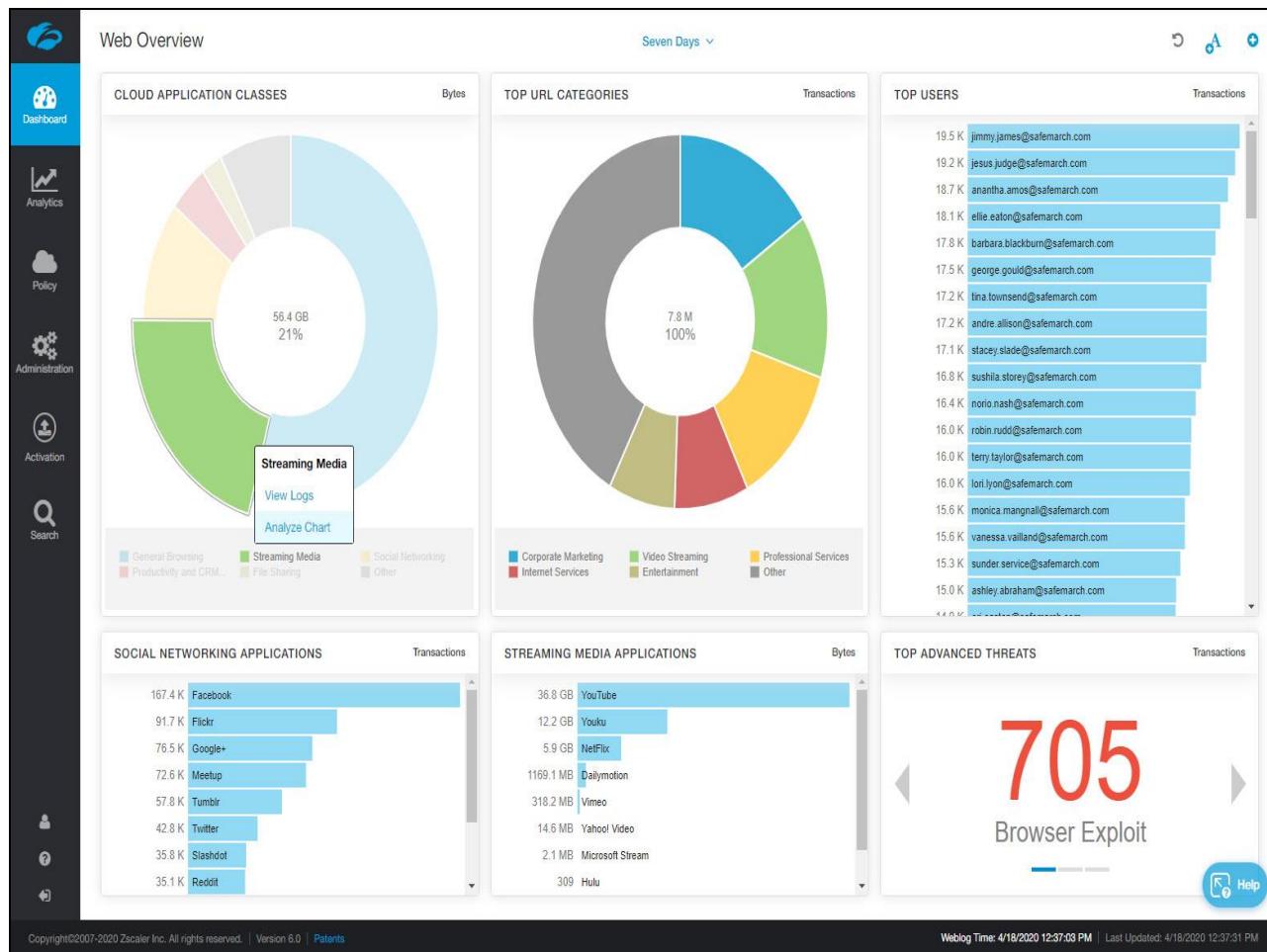
Slide 81 - Slide 81



Slide notes

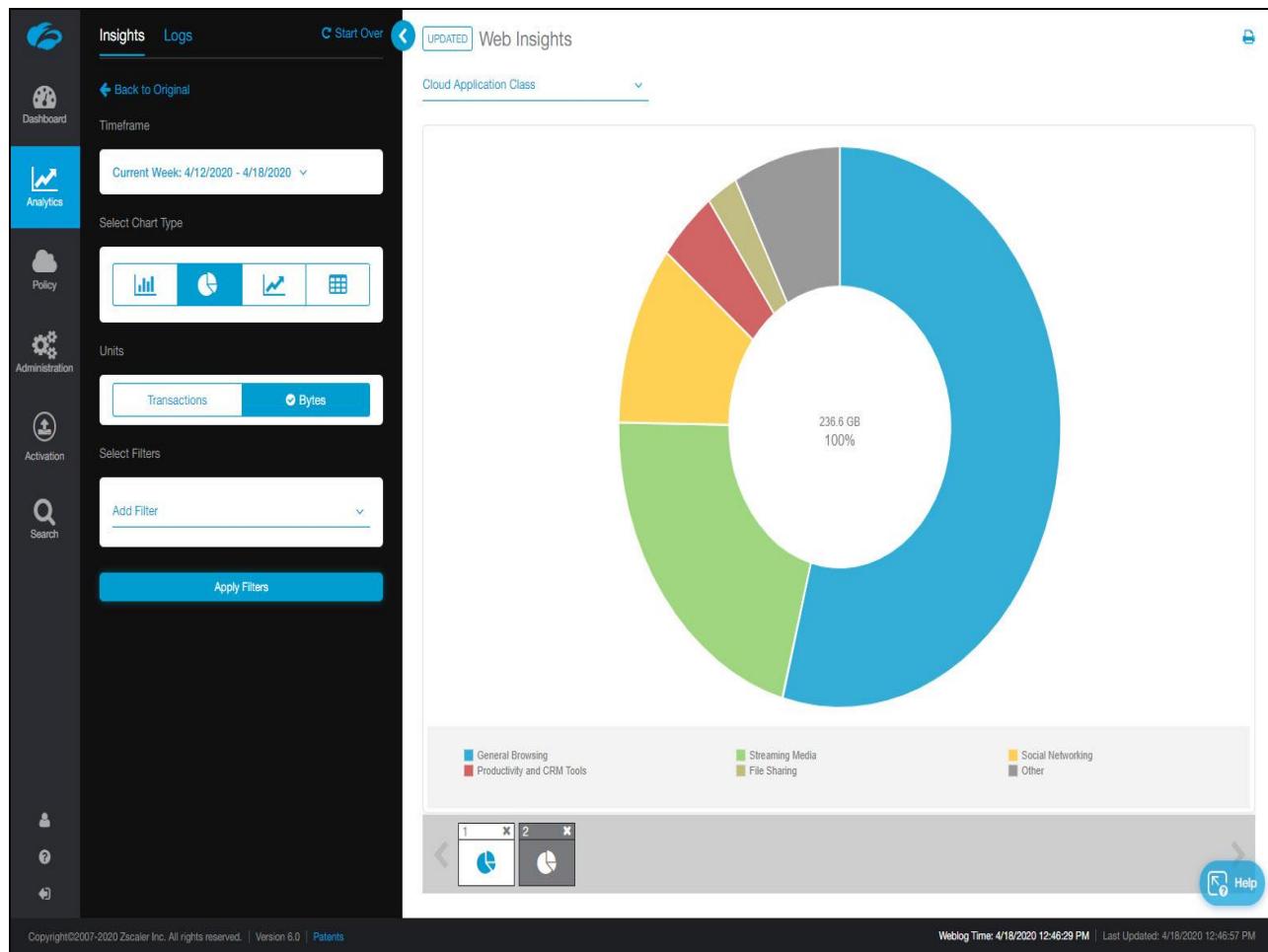
You have the option to view logs to see information such as what users are accessing sites under this application class or analyze the chart for further detail. Click on **Analyze Chart**.

Slide 82 - Slide 82



Slide notes

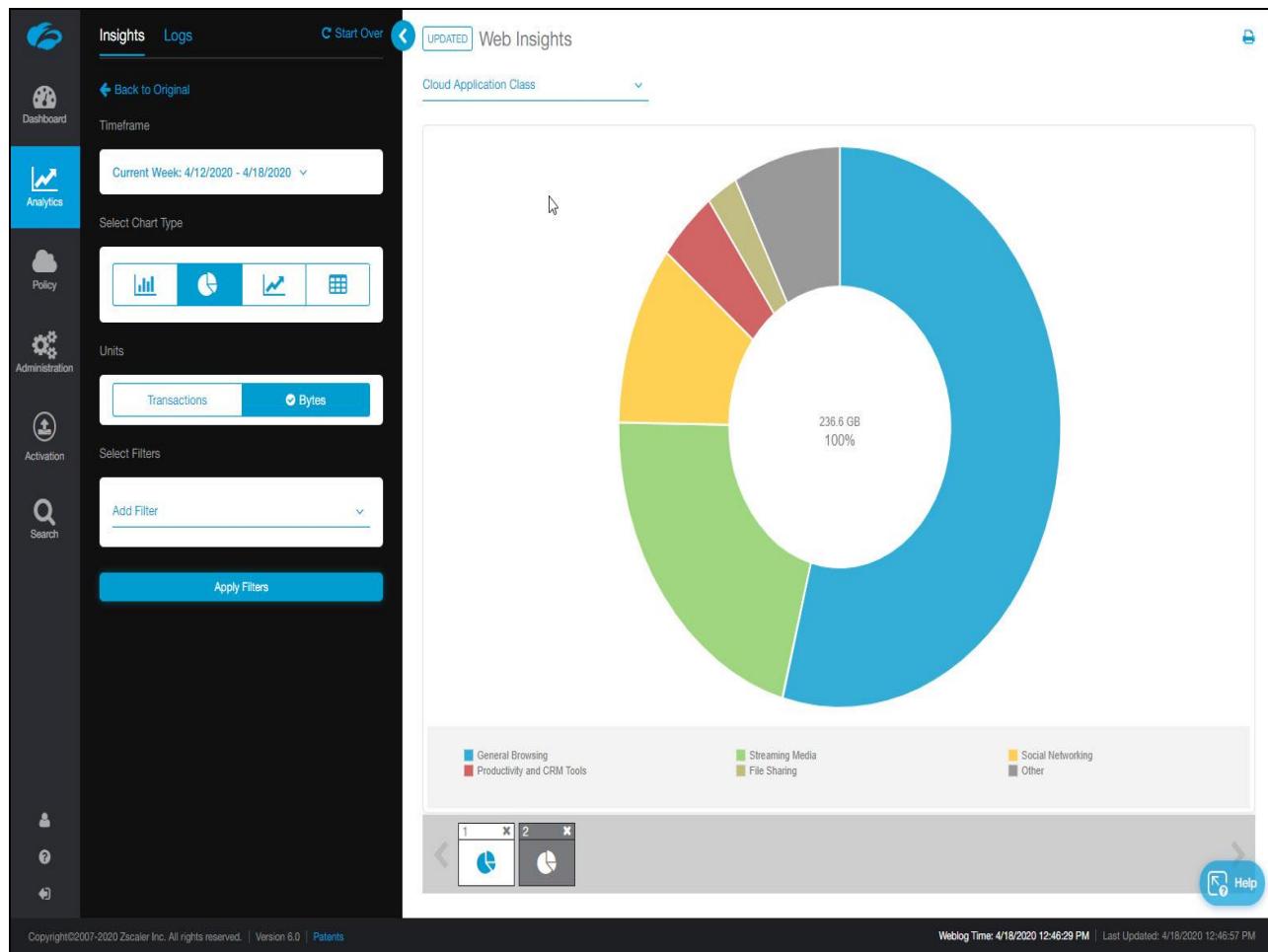
Slide 83 - Slide 83



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.

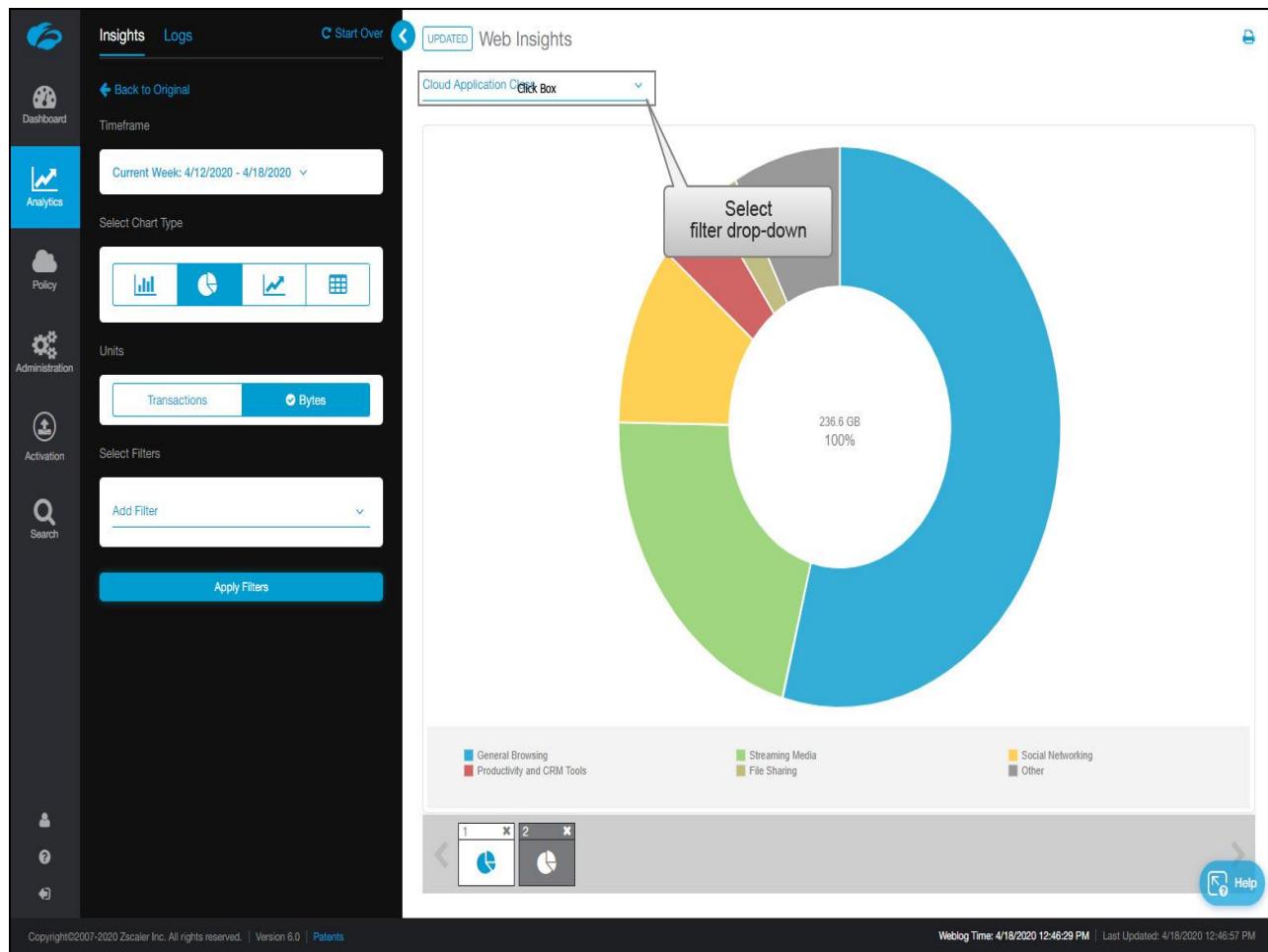
Slide 84 - Slide 84



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.

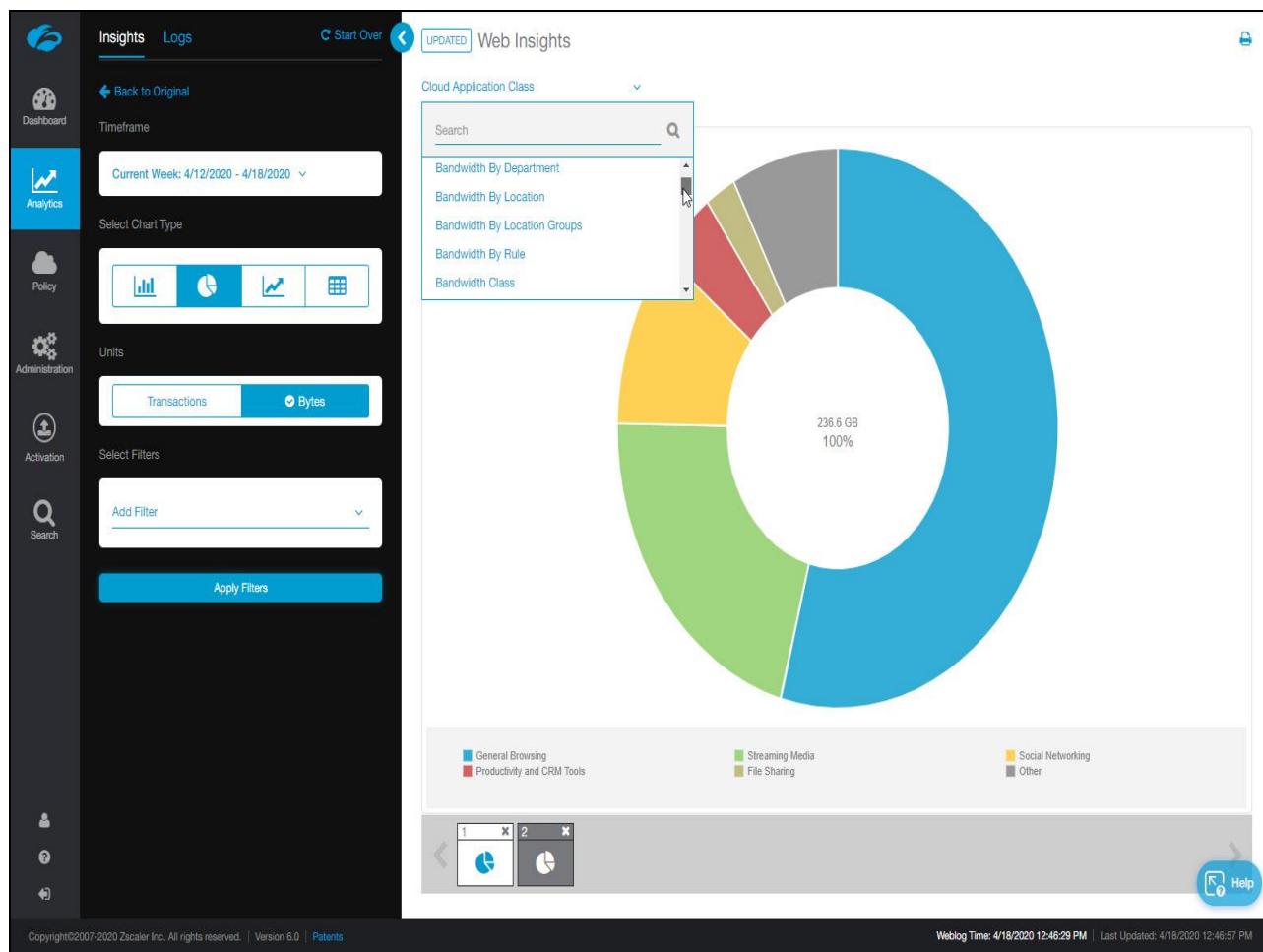
Slide 85 - Slide 85



Slide notes

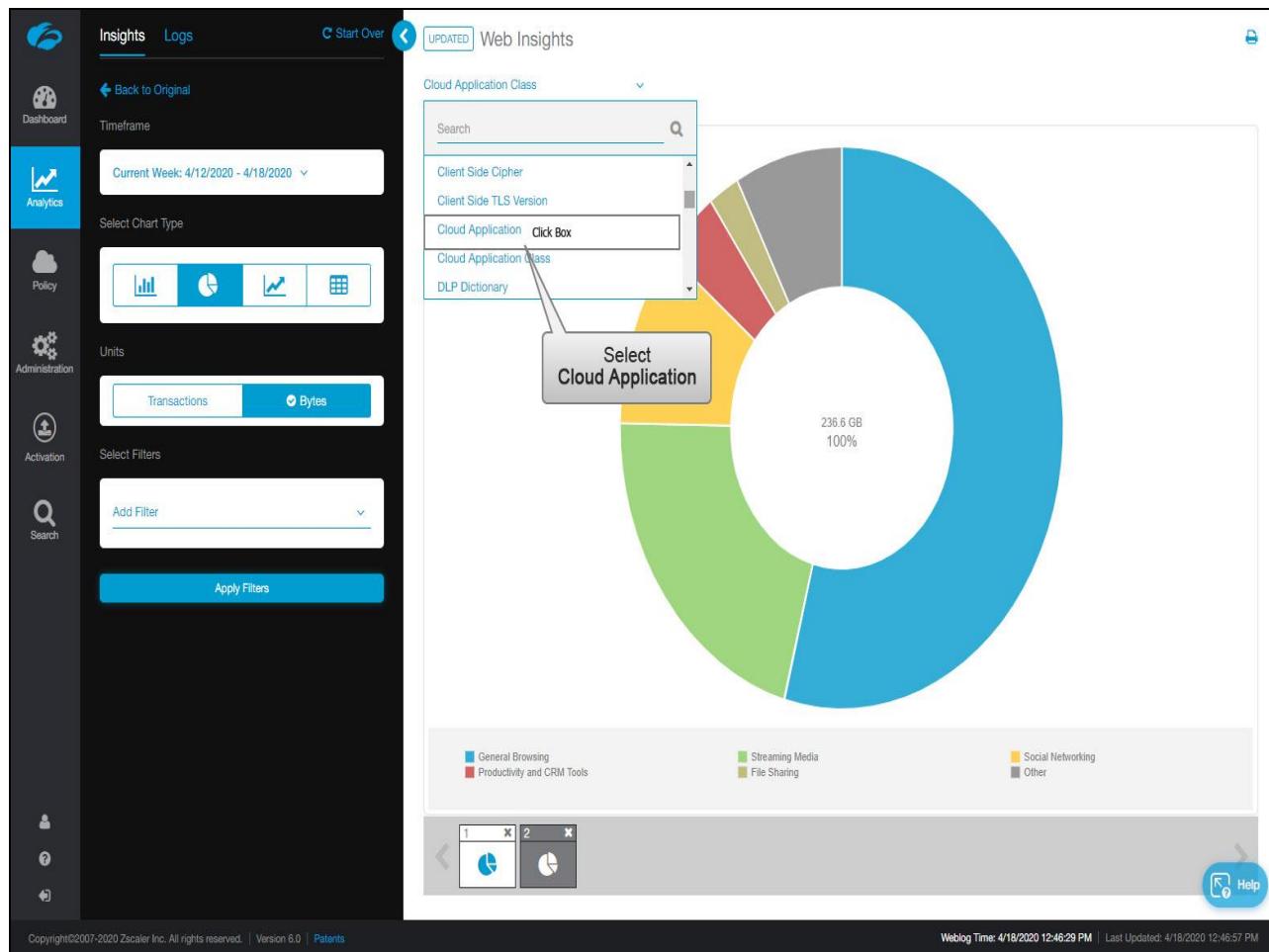
Click on the filter drop down.

Slide 86 - Slide 86



Slide notes

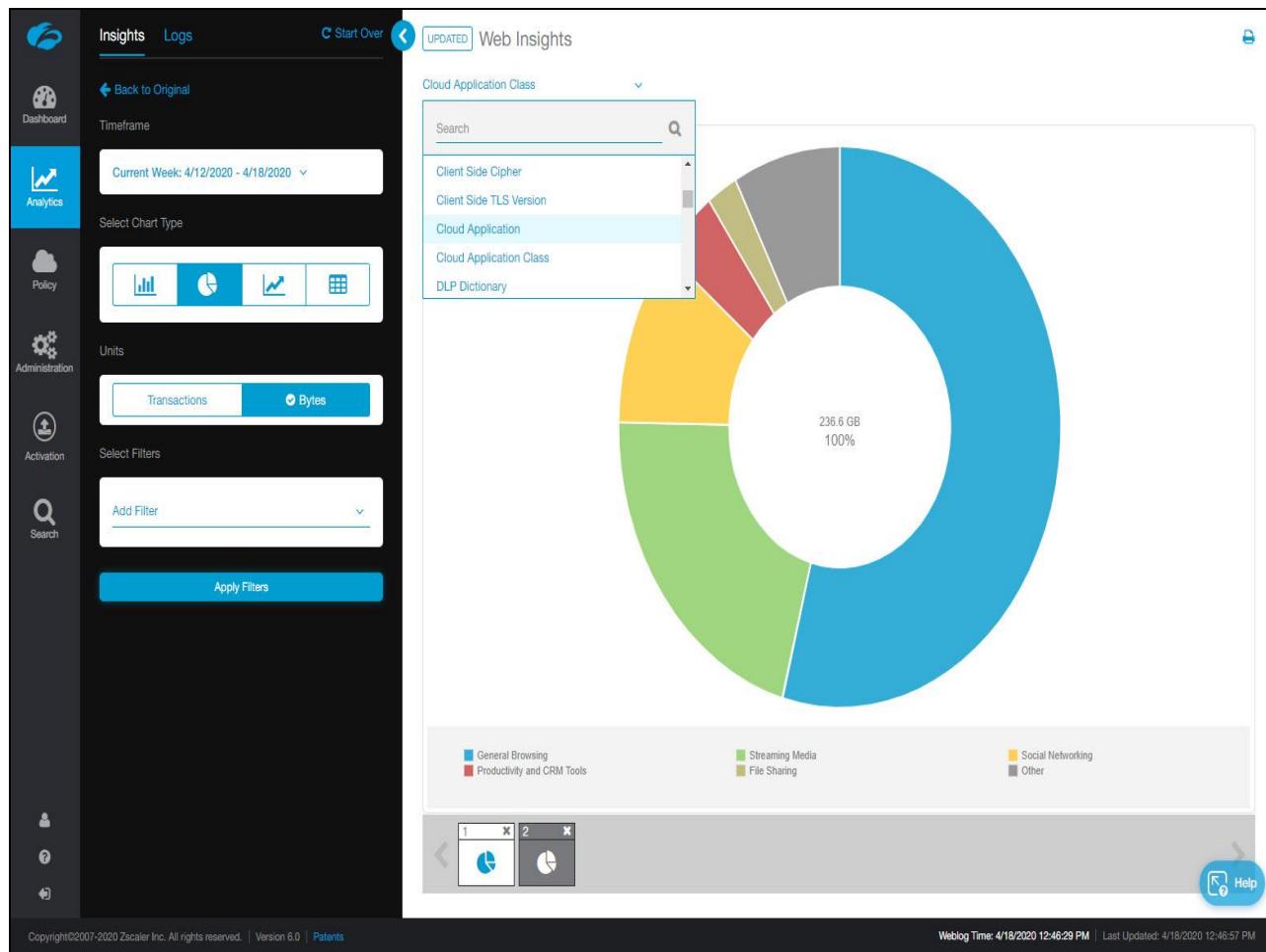
Slide 87 - Slide 87



Slide notes

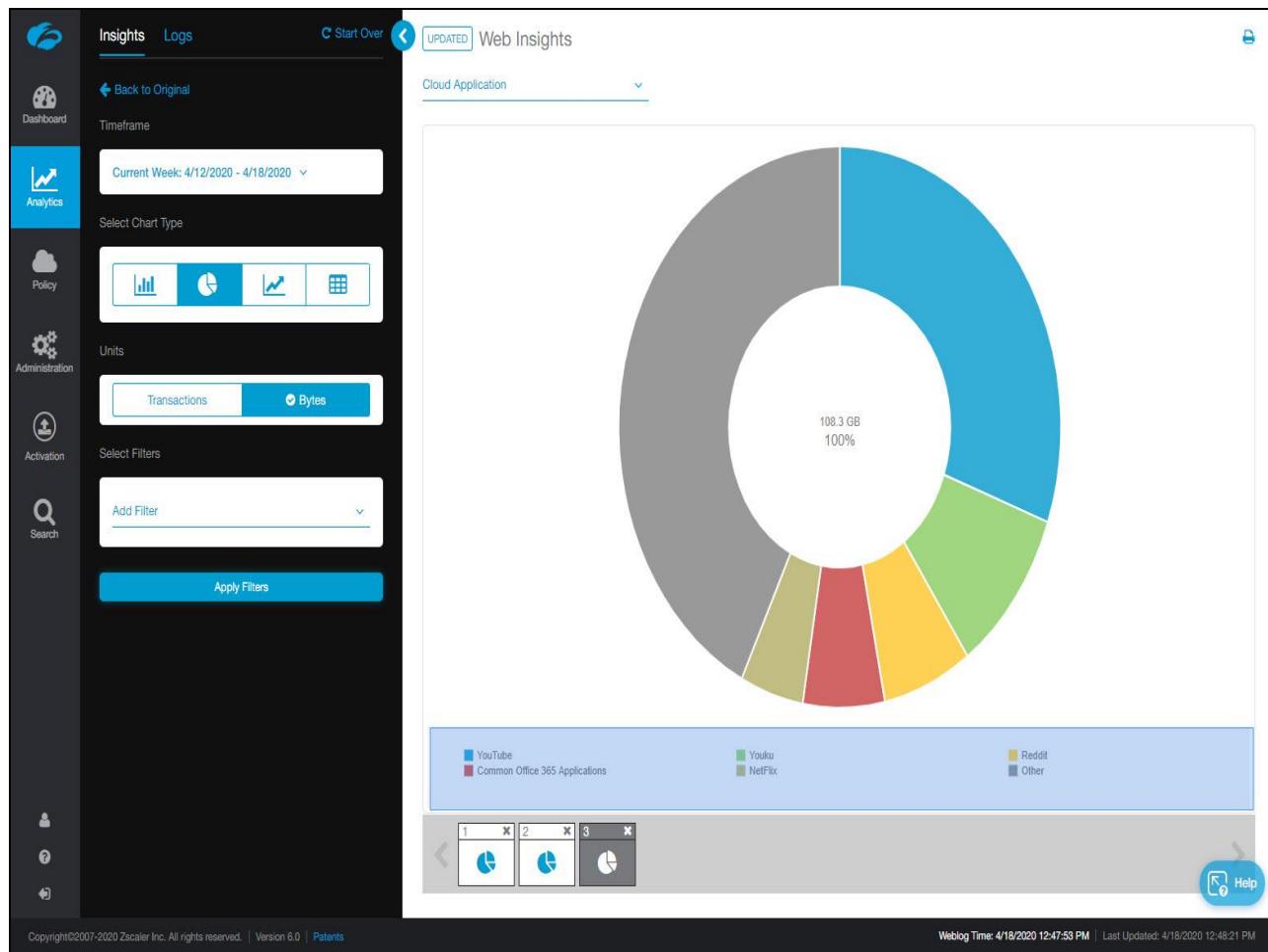
And select “Cloud Application”.

Slide 88 - Slide 88



Slide notes

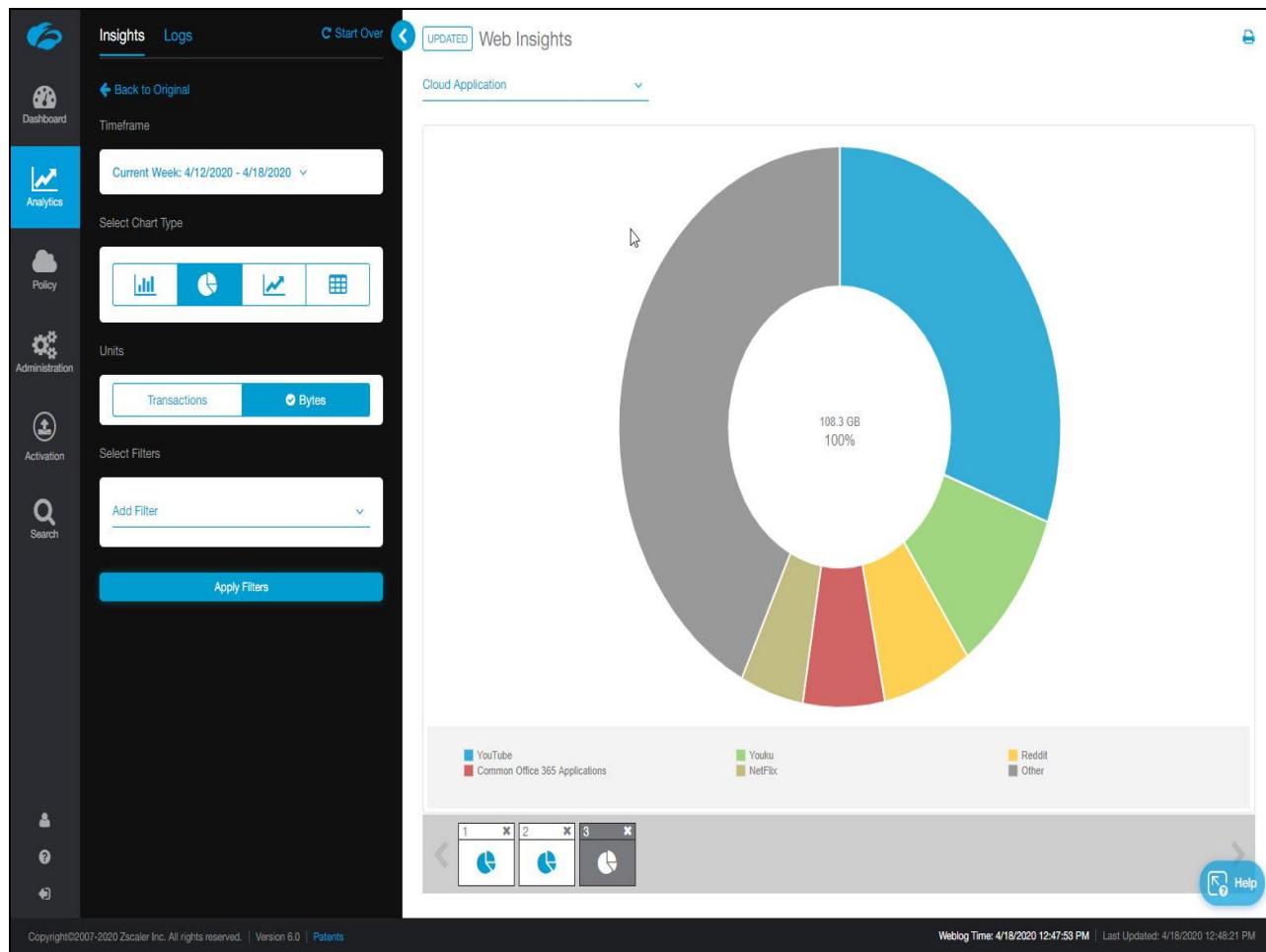
Slide 89 - Slide 89



Slide notes

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

Slide 90 - Slide 90

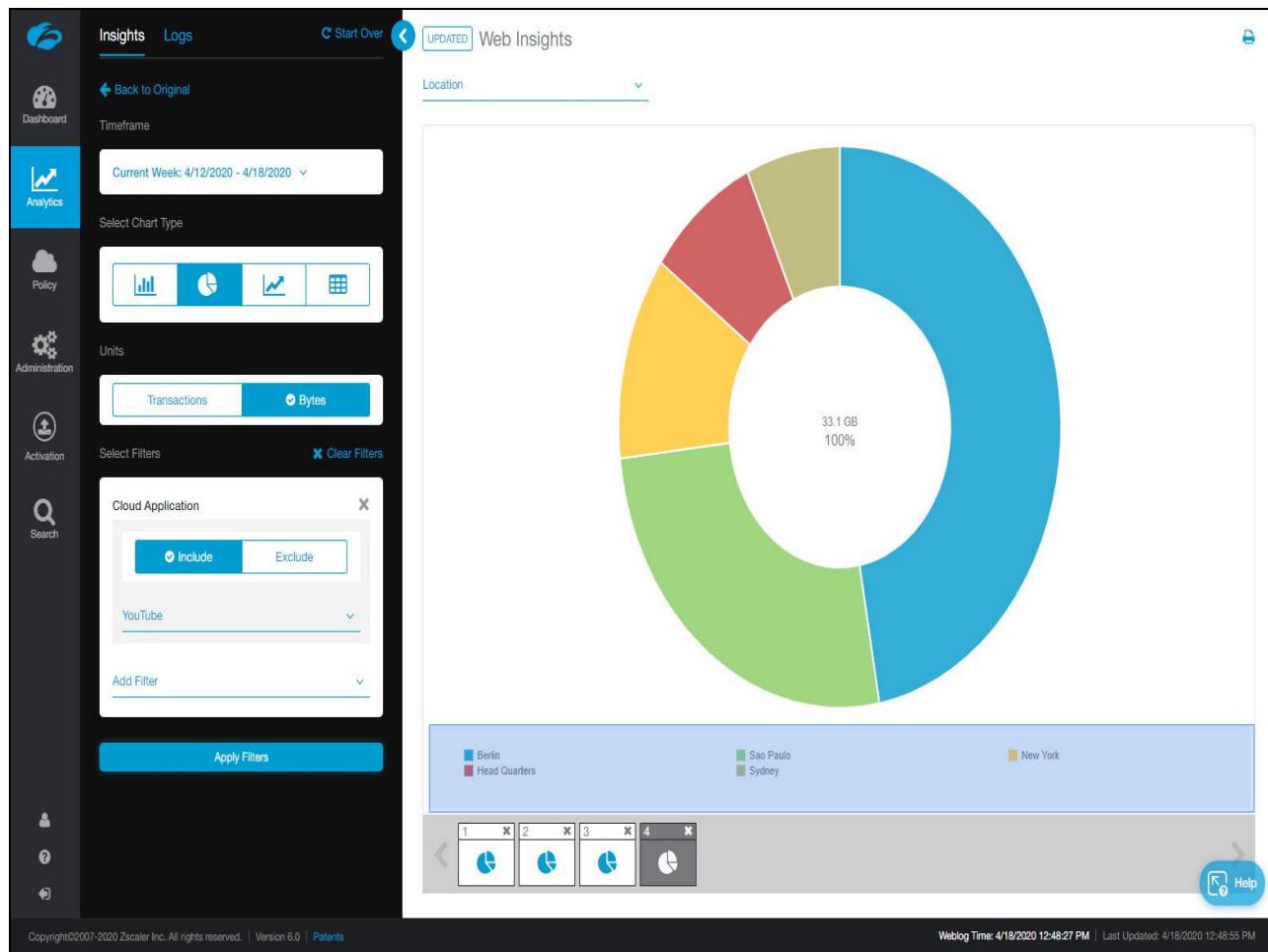


Slide notes

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.

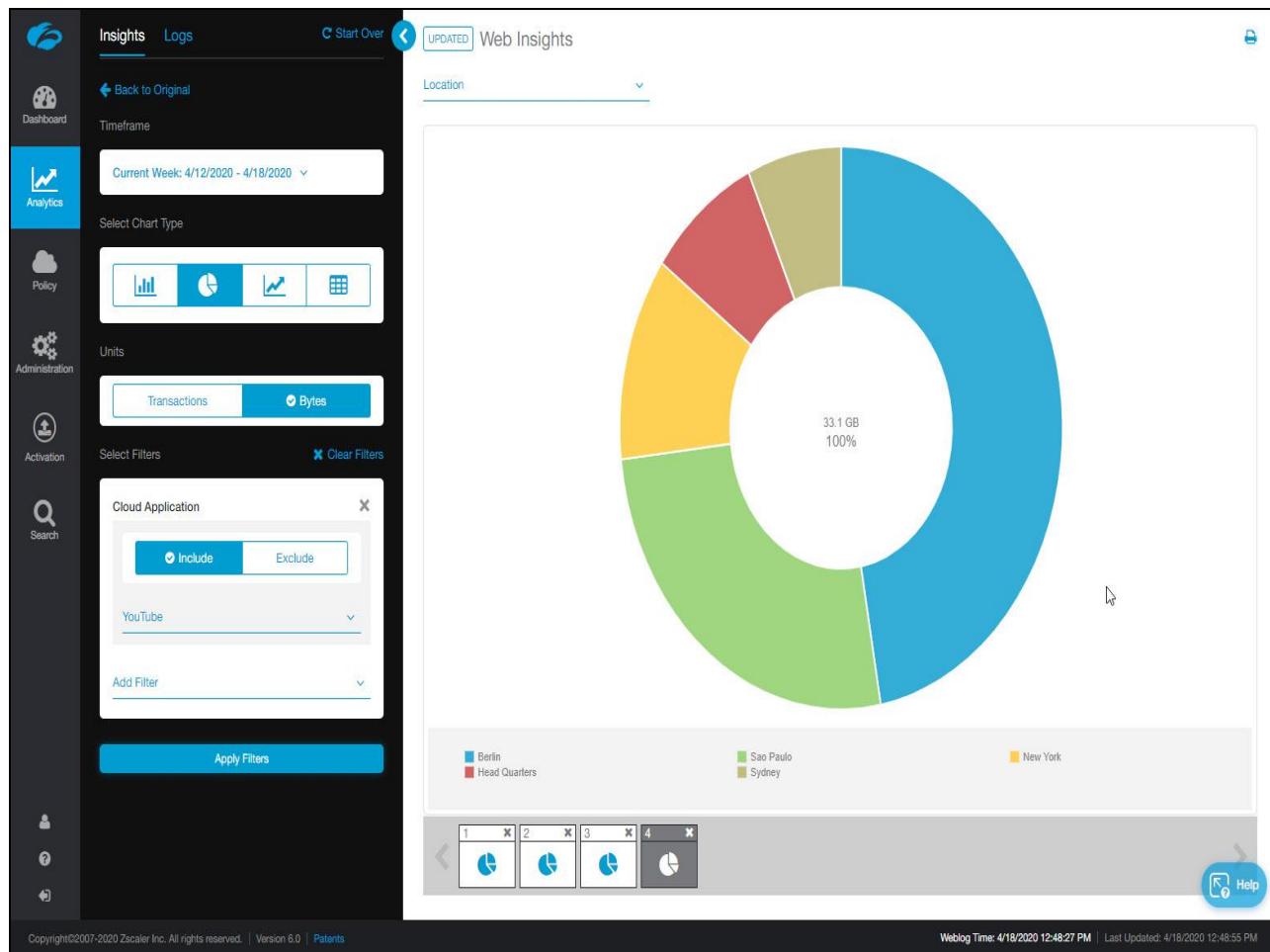
Slide 91 - Slide 91



Slide notes

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

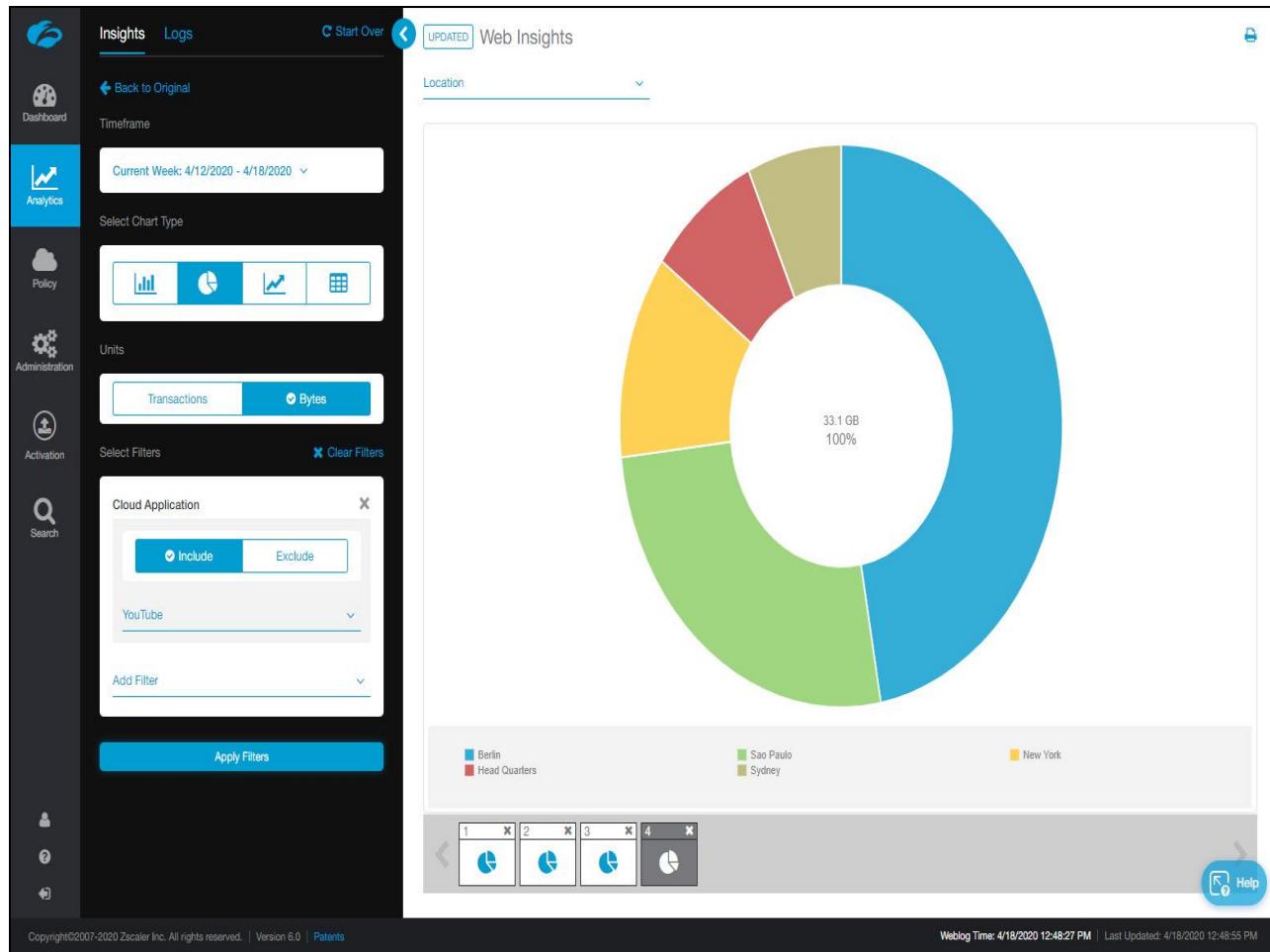
Slide 92 - Slide 92



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.

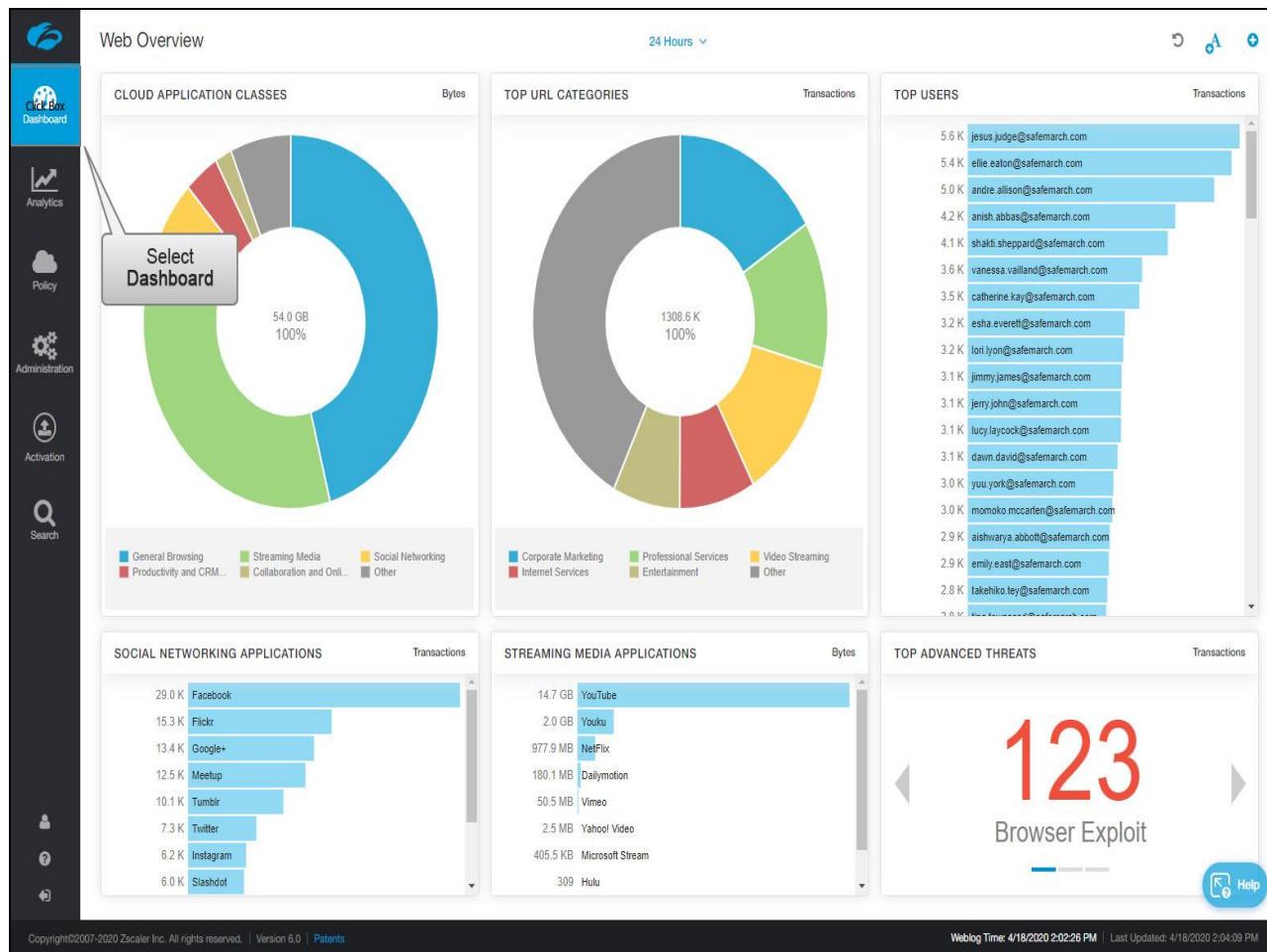
These are all options you can configure under Policy configuration which is covered in a separate module. For now, let's assume that blocking YouTube companywide is the right solution. I will configure this policy off screen, and we will look at the results in just a moment.

Slide 94 - Slide 94



Slide notes

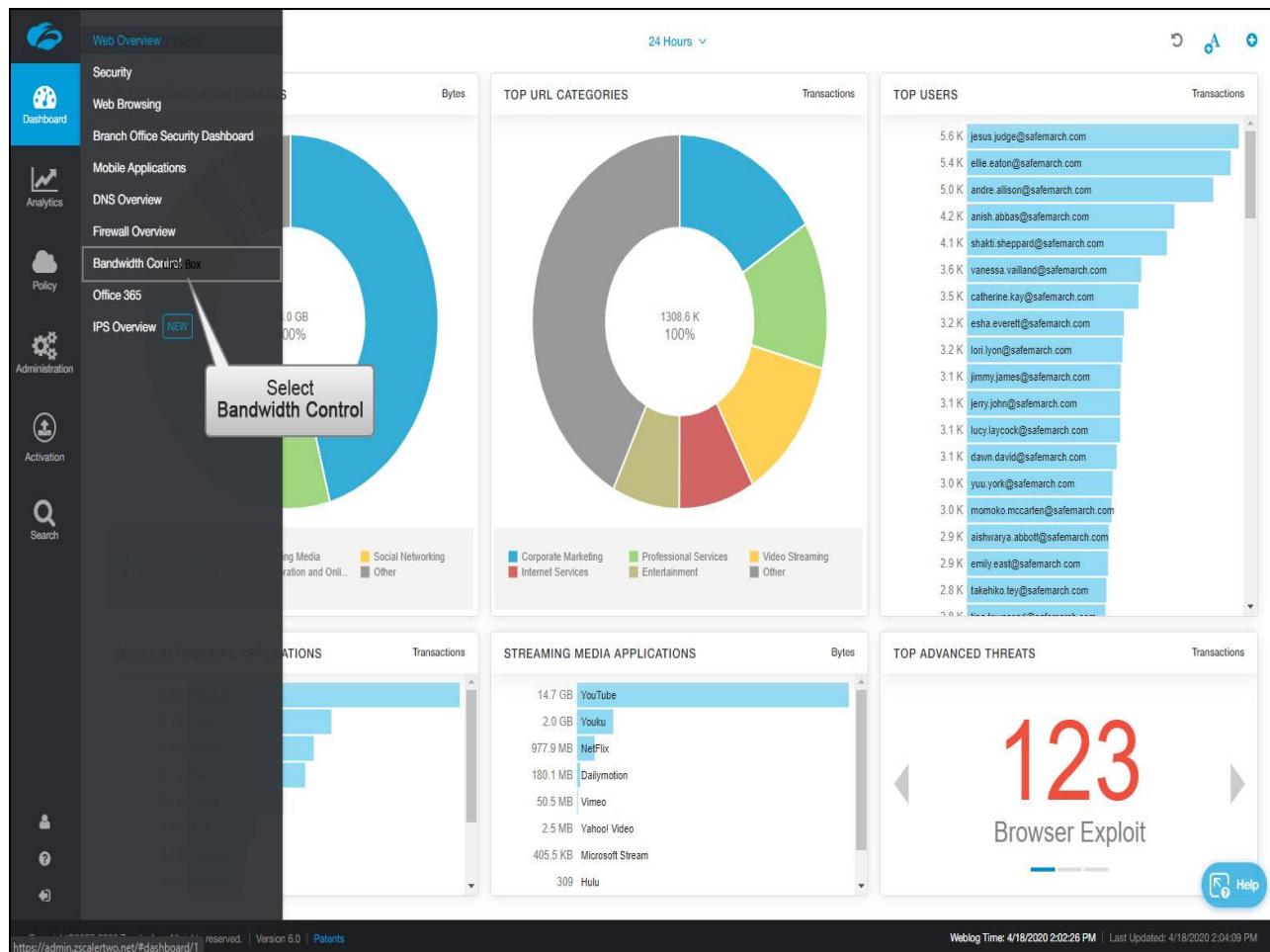
Slide 95 - Slide 95



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.

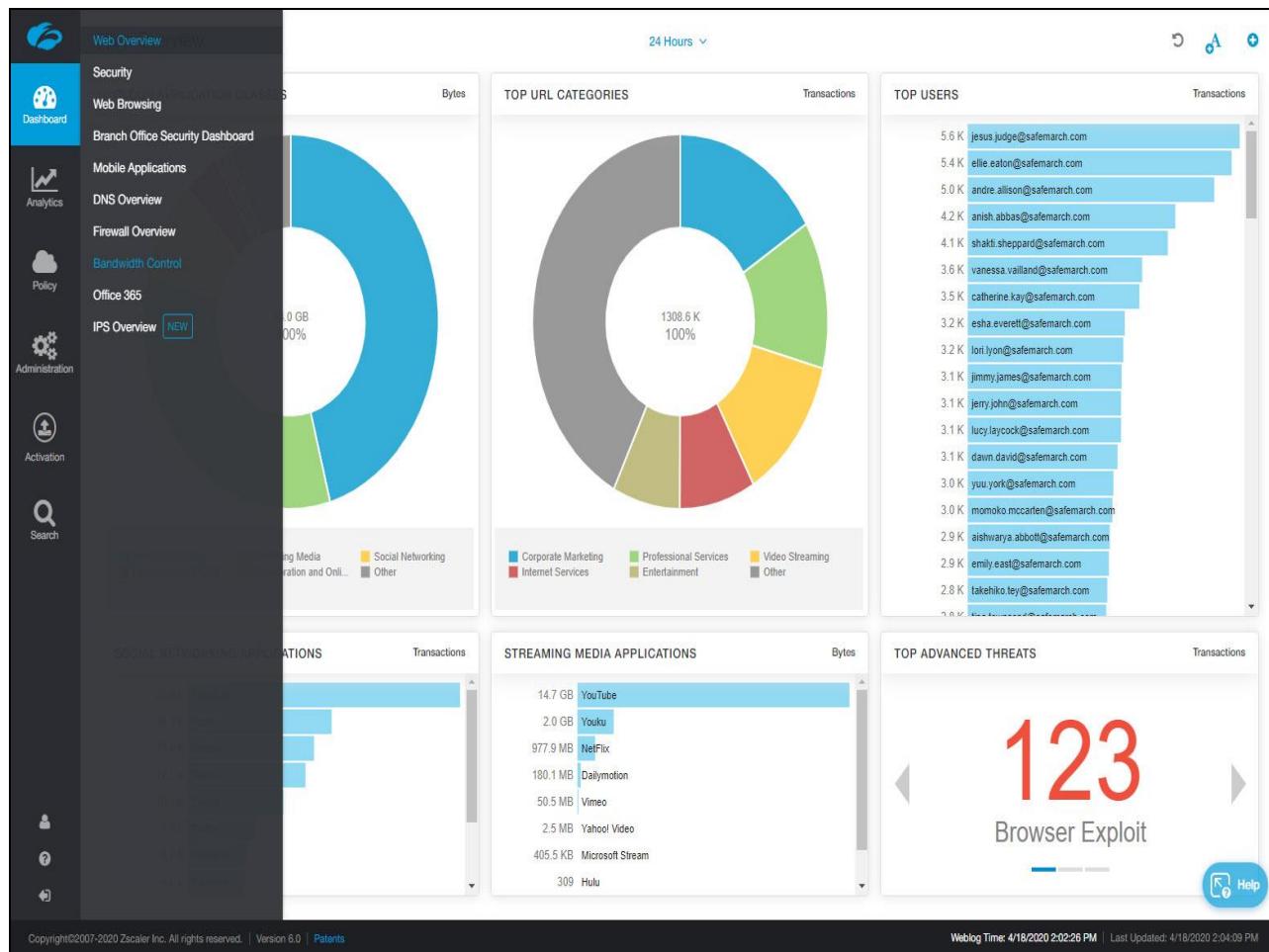
Slide 96 - Slide 96



Slide notes

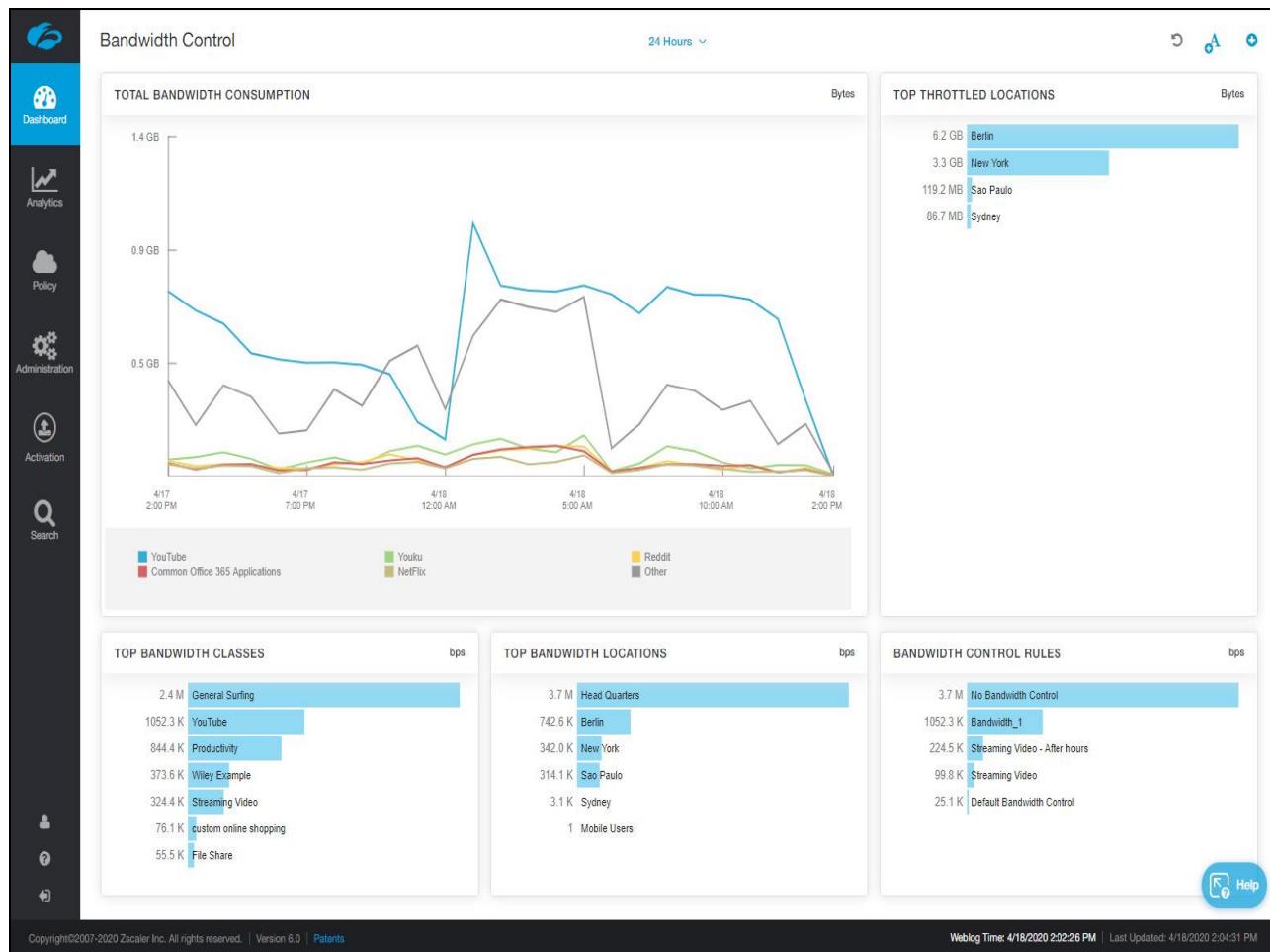
And select **Bandwidth Control**.

Slide 97 - Slide 97



Slide notes

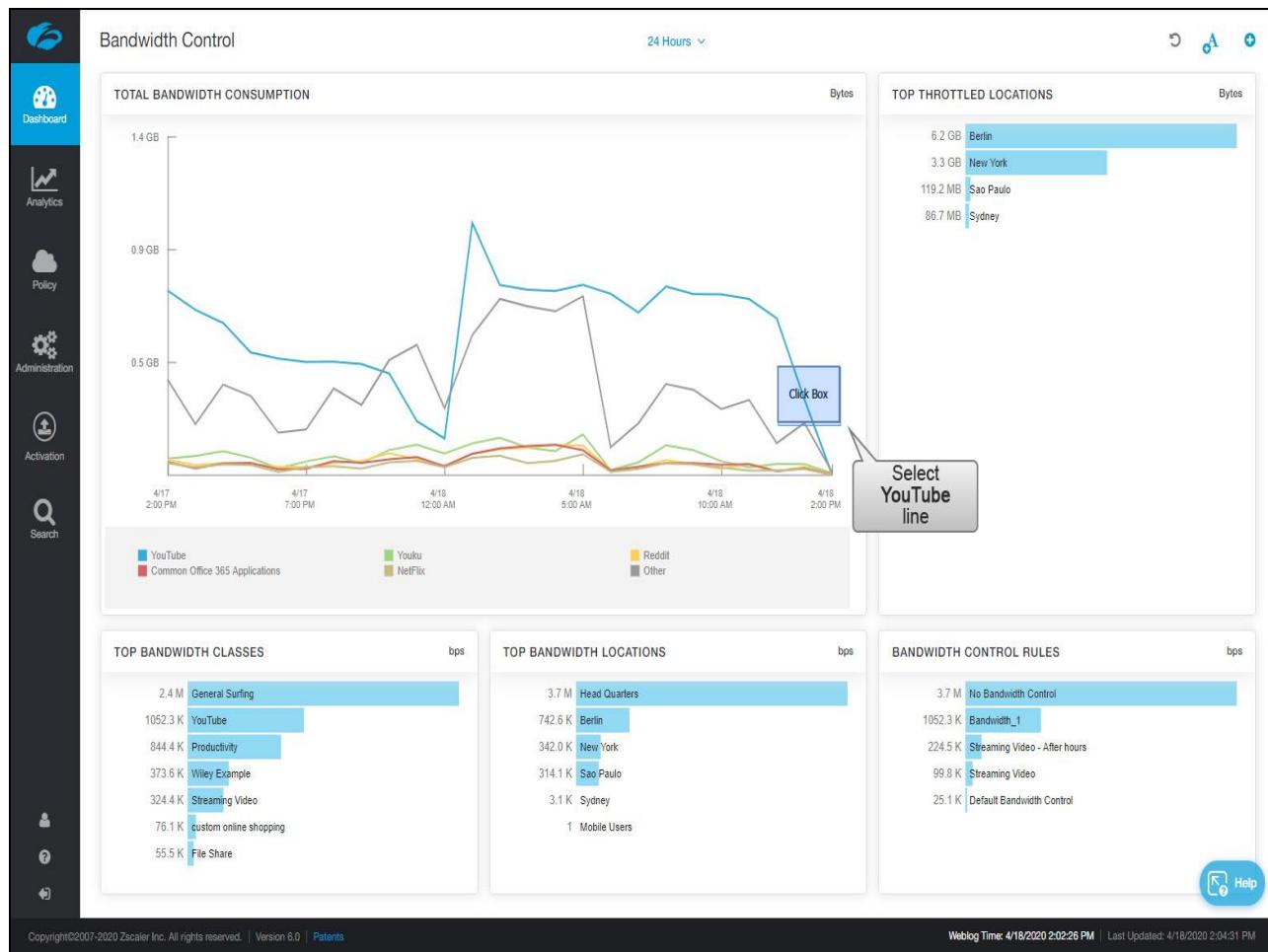
Slide 98 - Slide 98



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

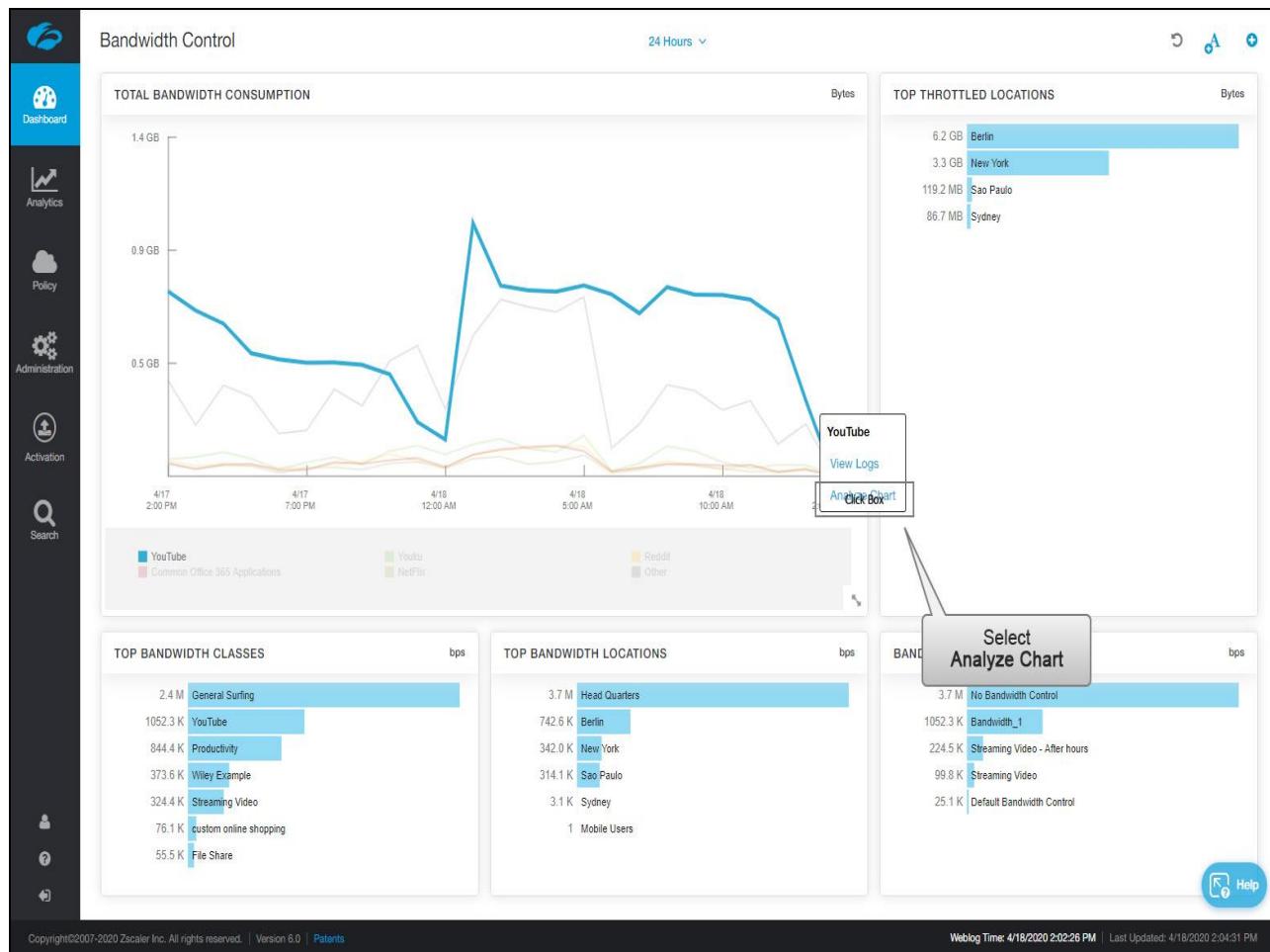


Slide notes

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.

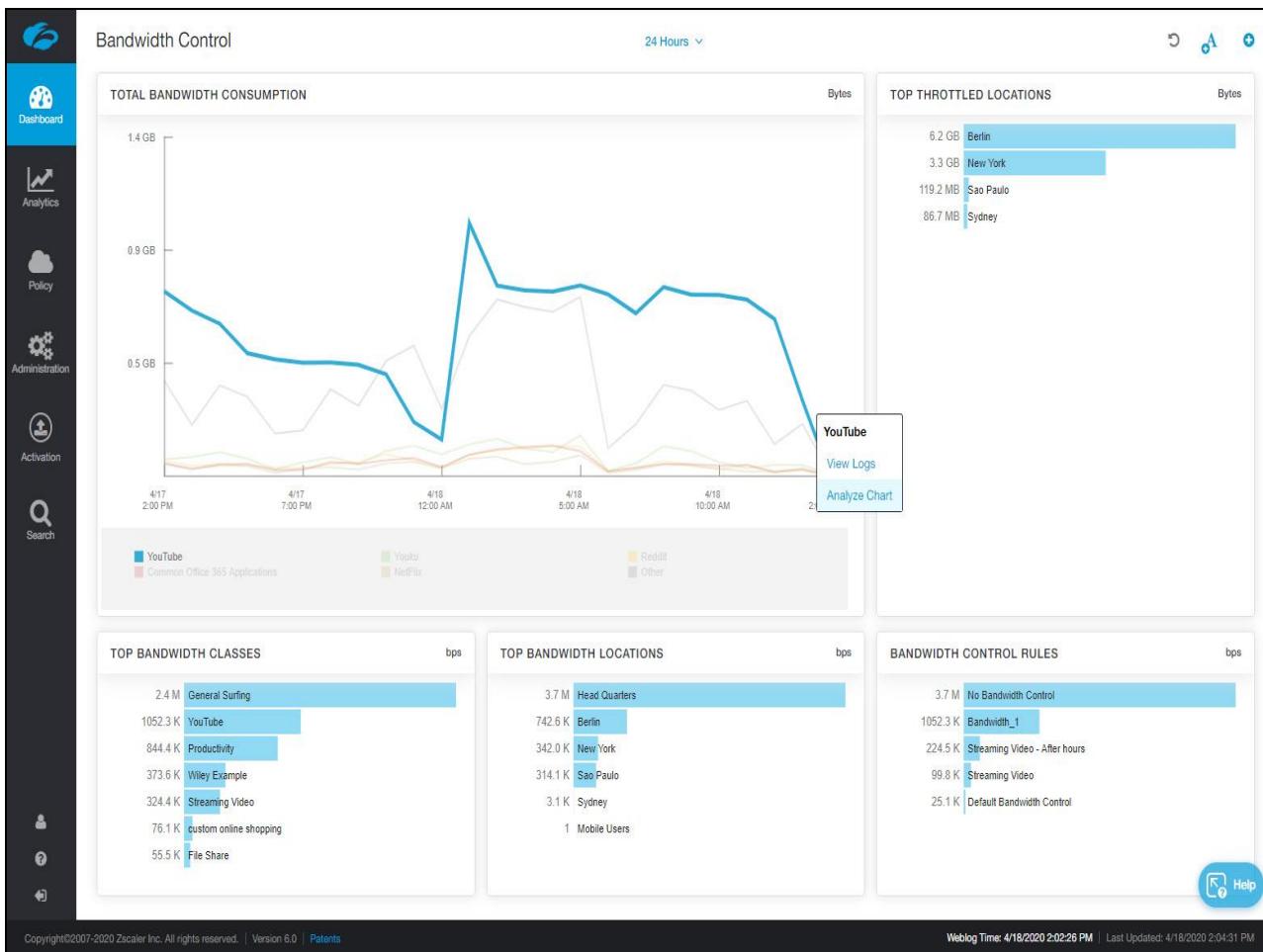
Slide 100 - Slide 100



Slide notes

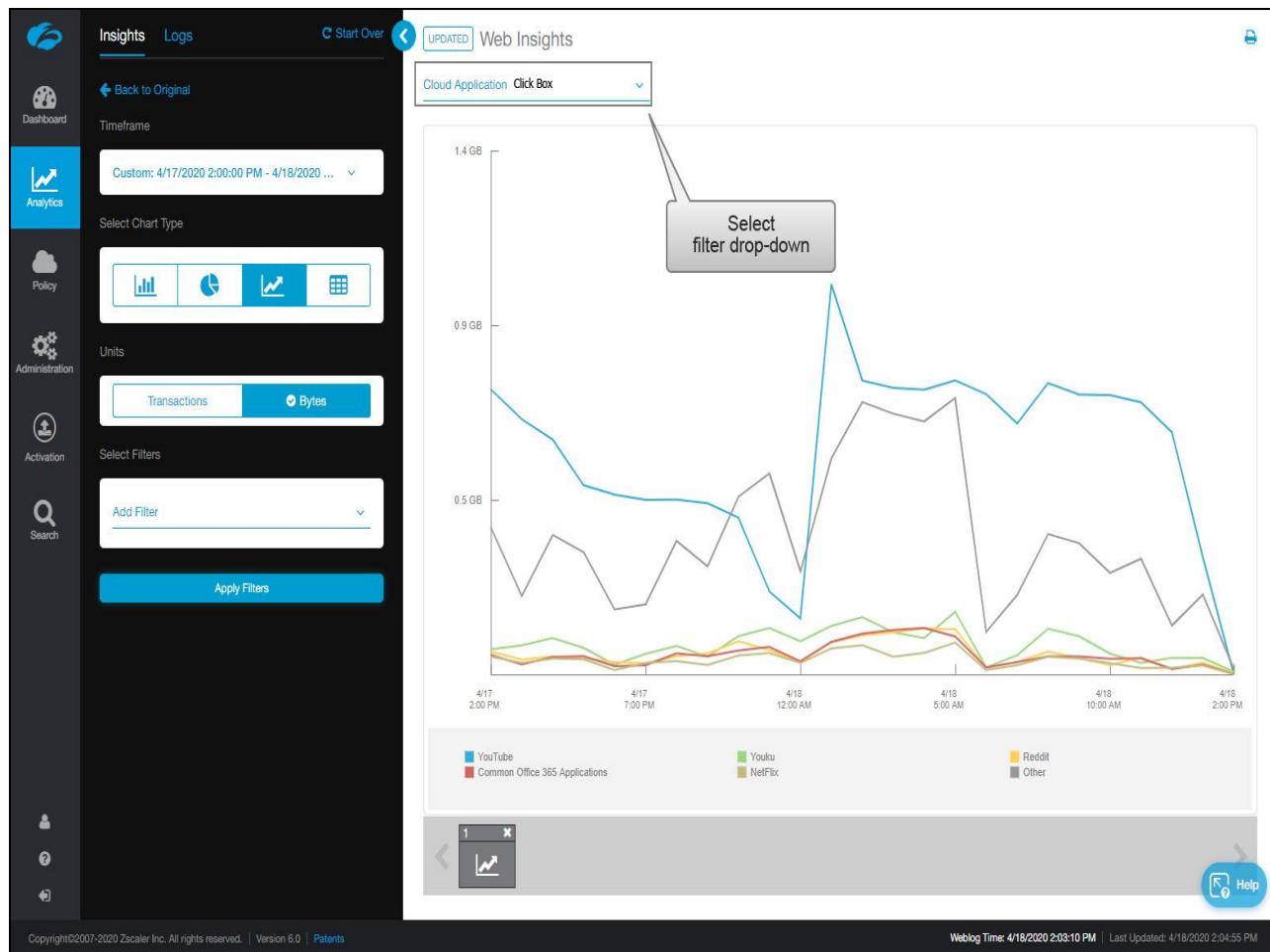
Select **Analyze Chart**.

Slide 101 - Slide 101



Slide notes

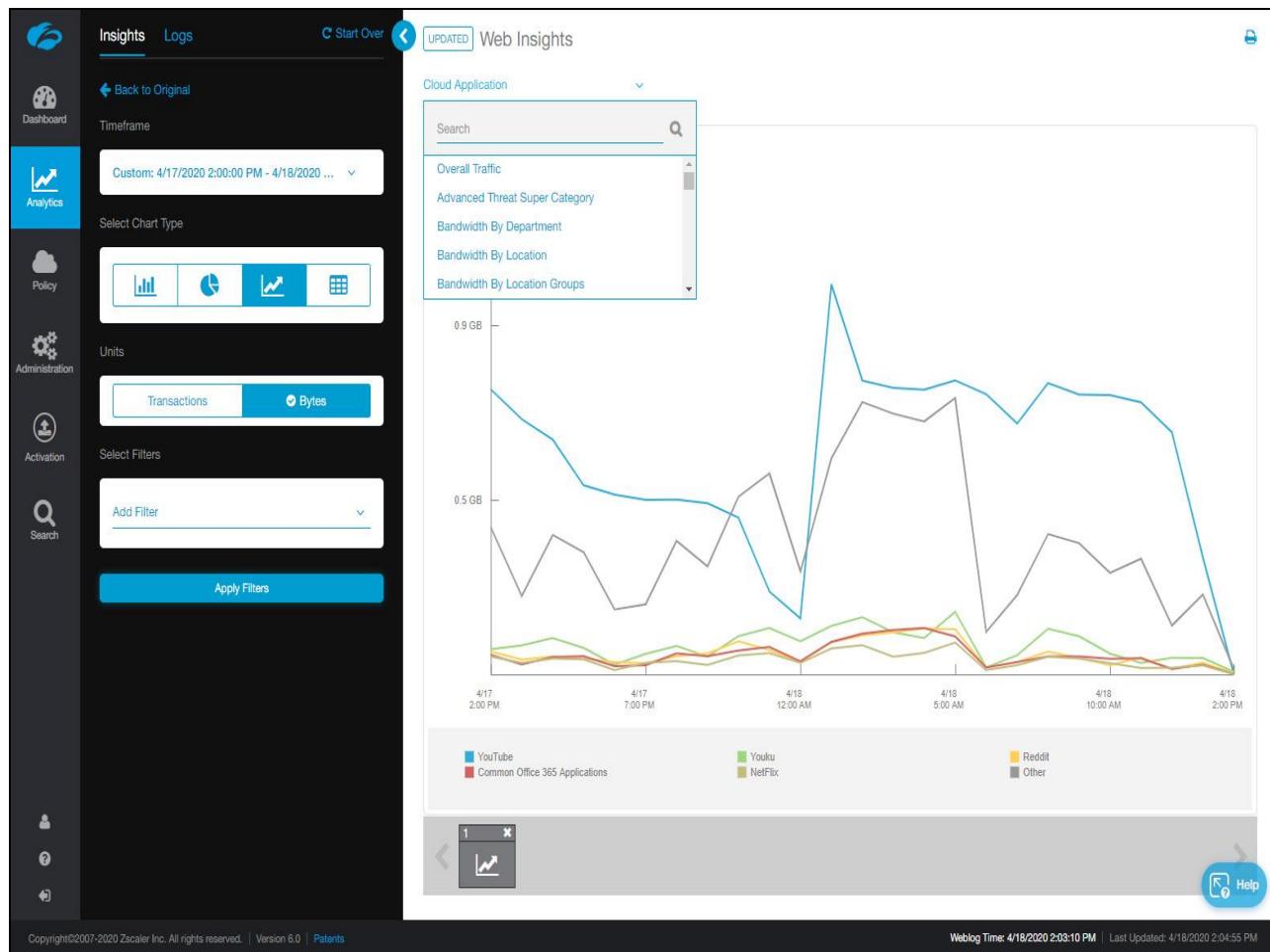
Slide 102 - Slide 102



Slide notes

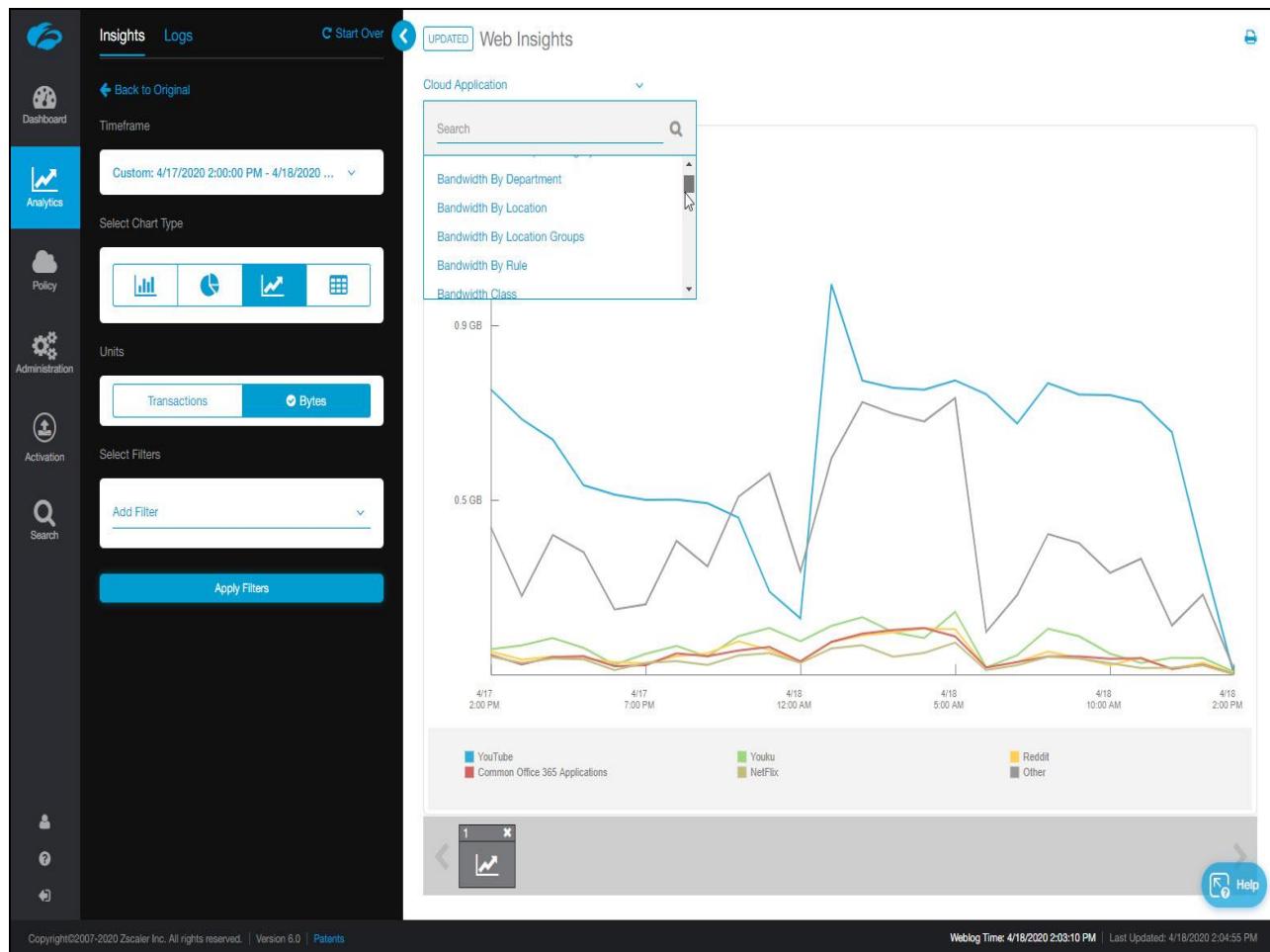
Select the filter drop-down.

Slide 103 - Slide 103



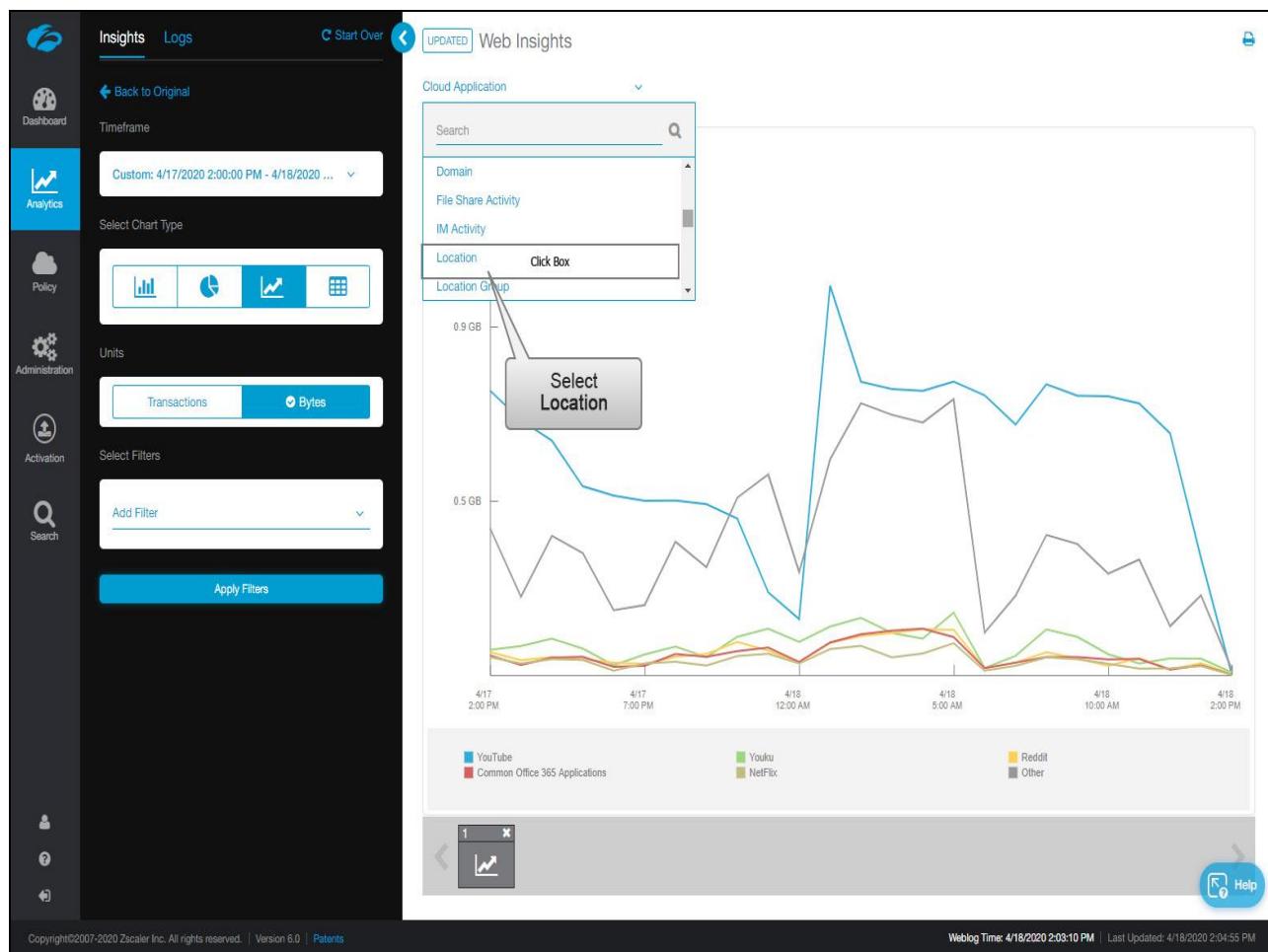
Slide notes

Slide 104 - Slide 104



Slide notes

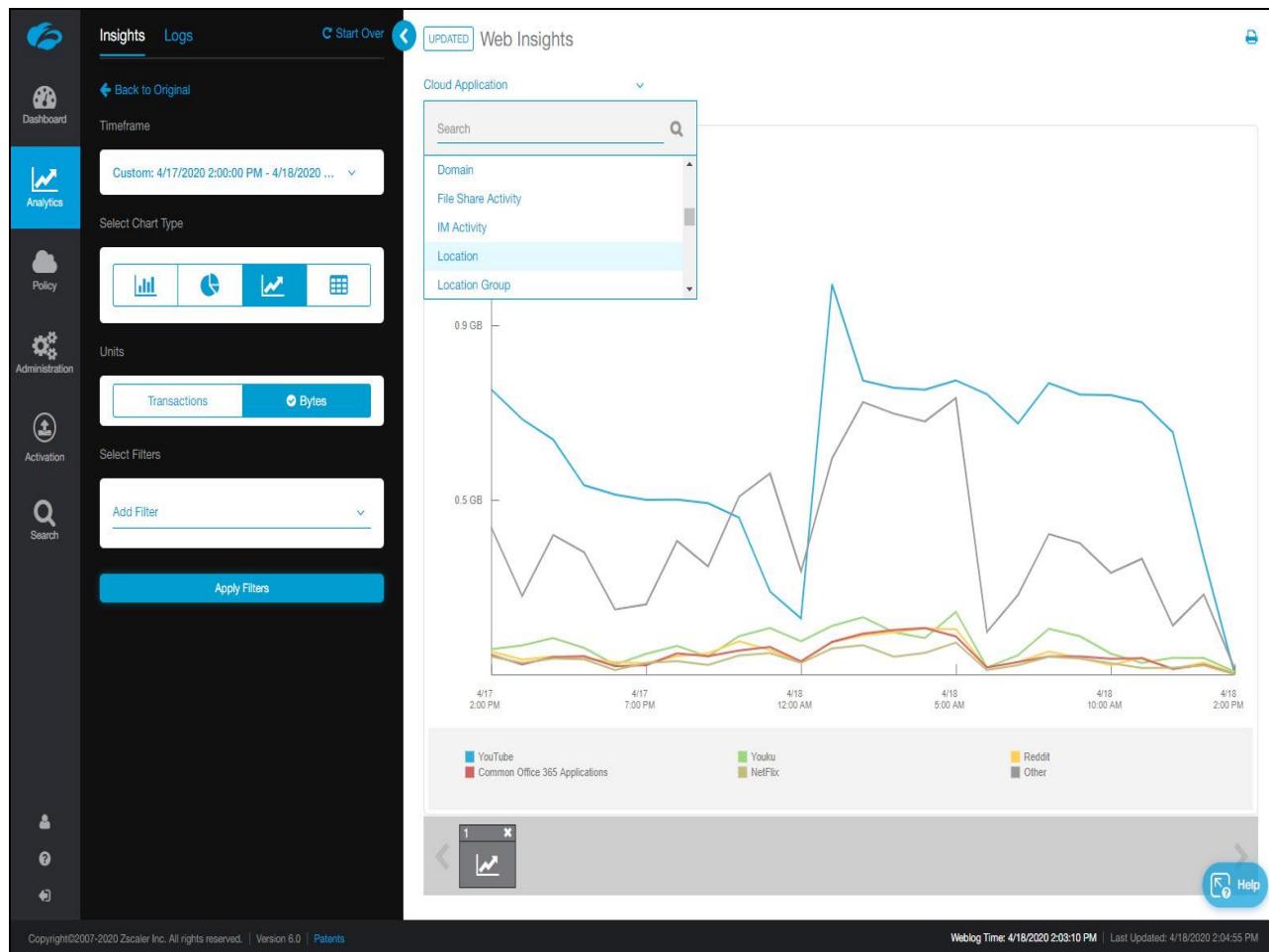
Slide 105 - Slide 105



Slide notes

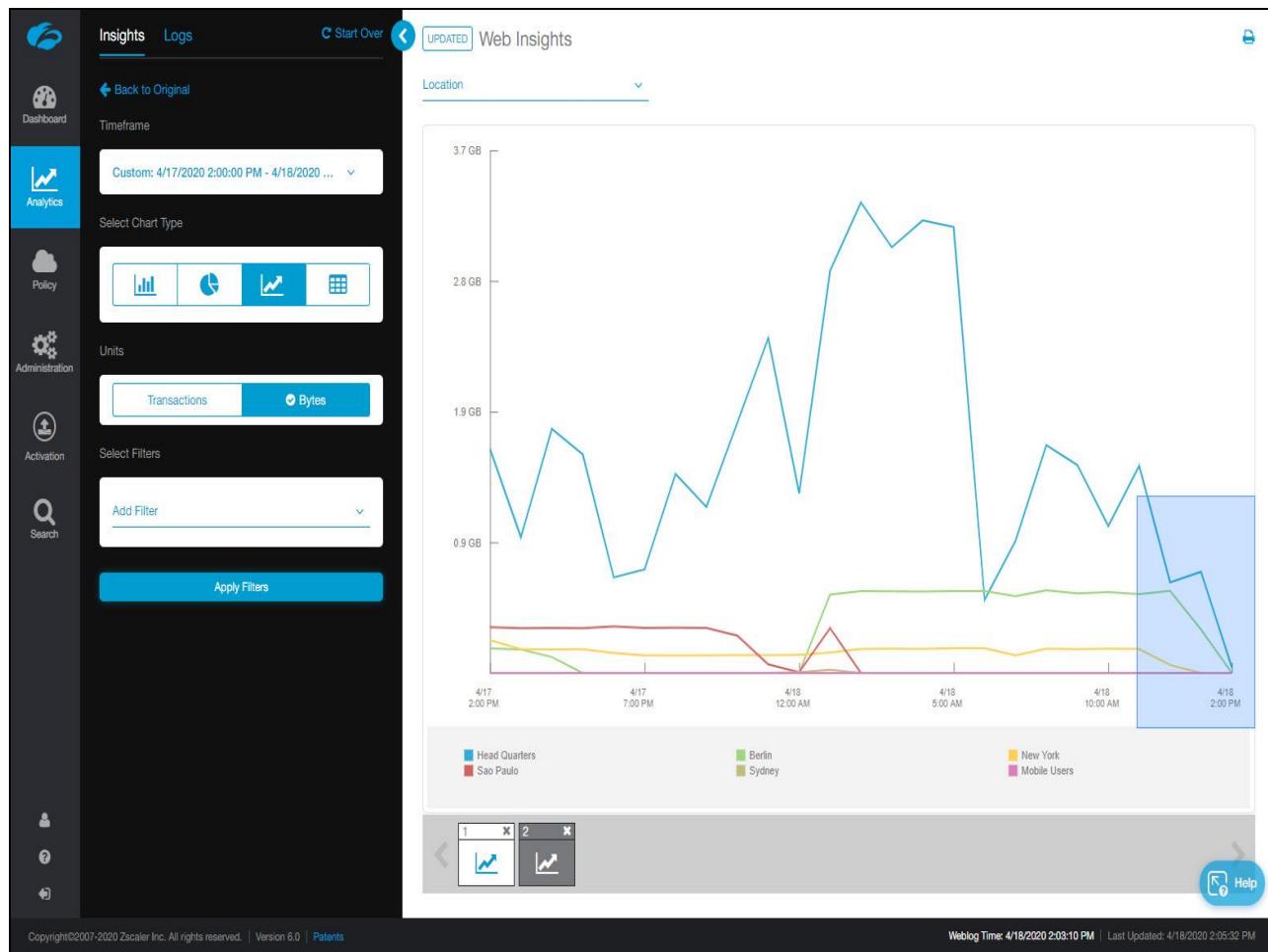
And select **Location**.

Slide 106 - Slide 106



Slide notes

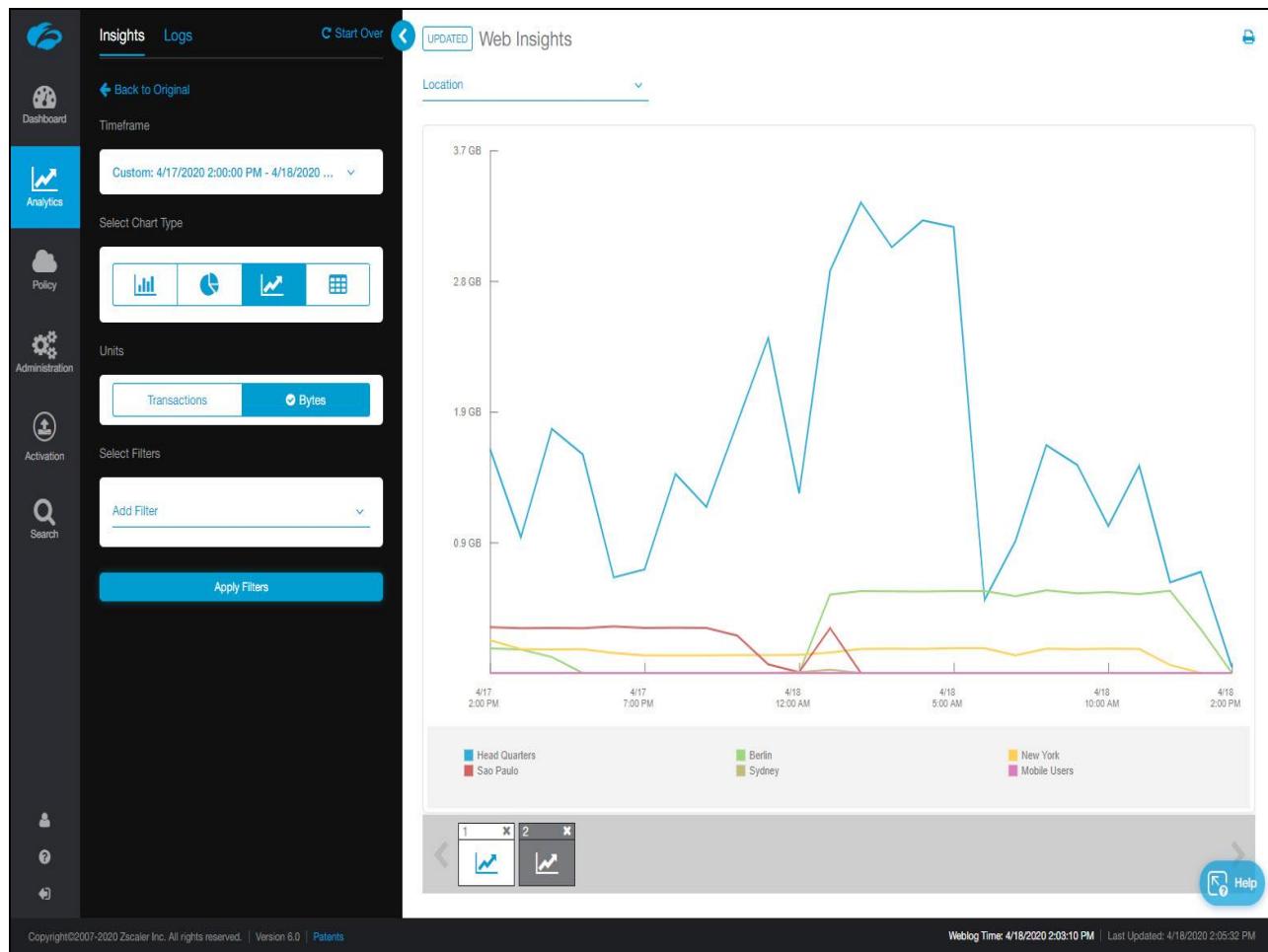
Slide 107 - Slide 107



Slide notes

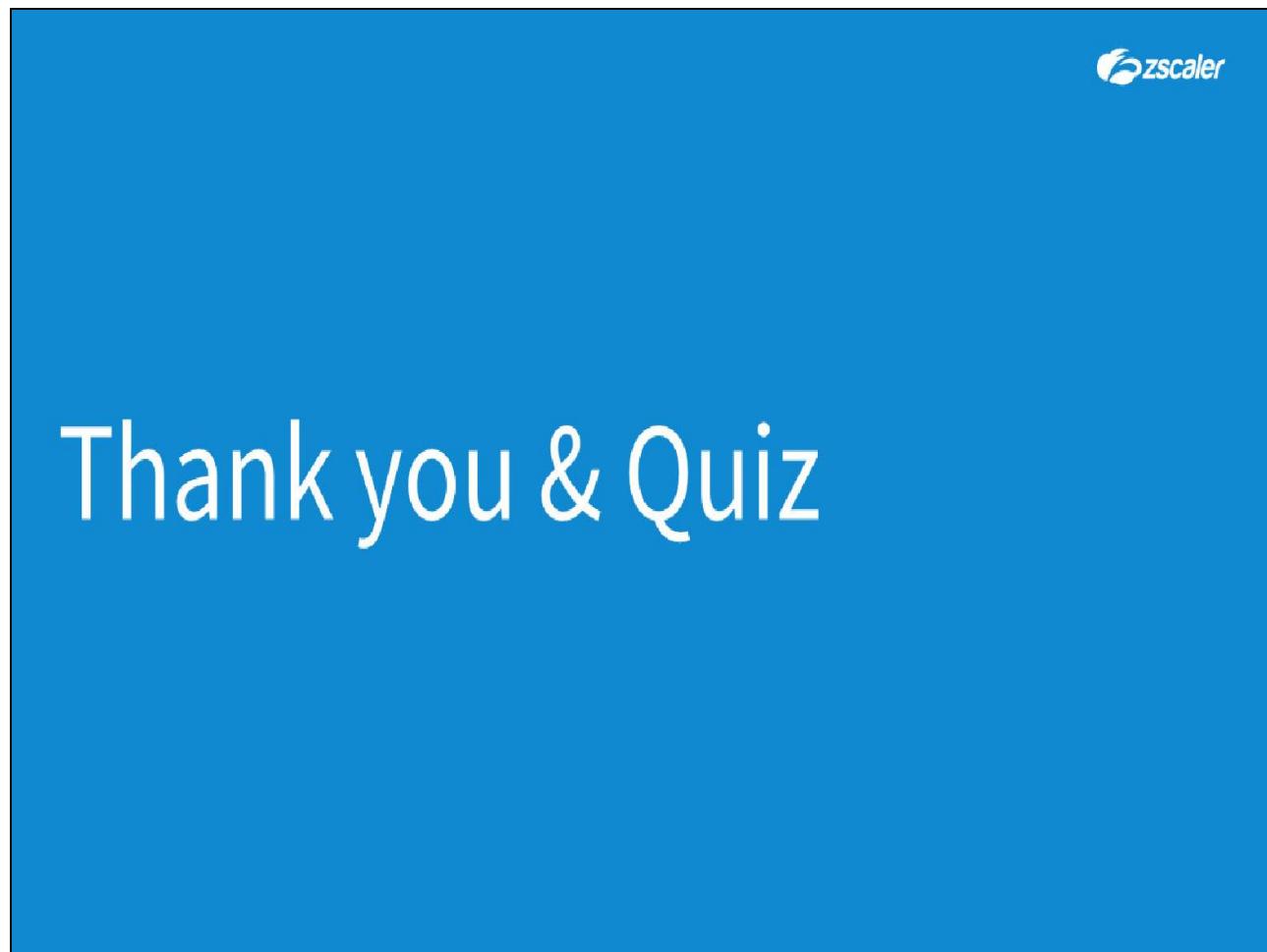
And you can see that YouTube traffic for all locations experienced a sharp drop off.

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.

