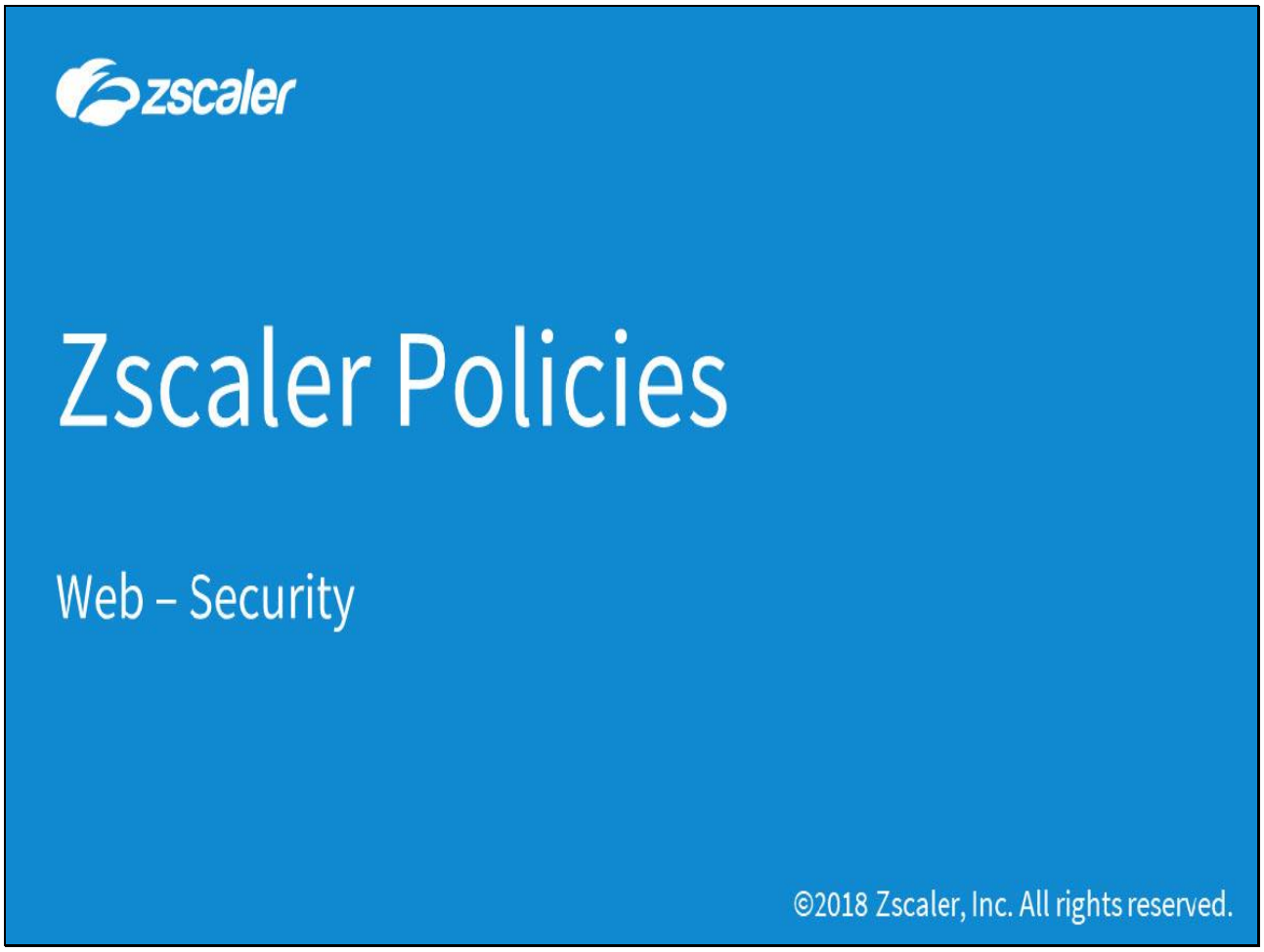
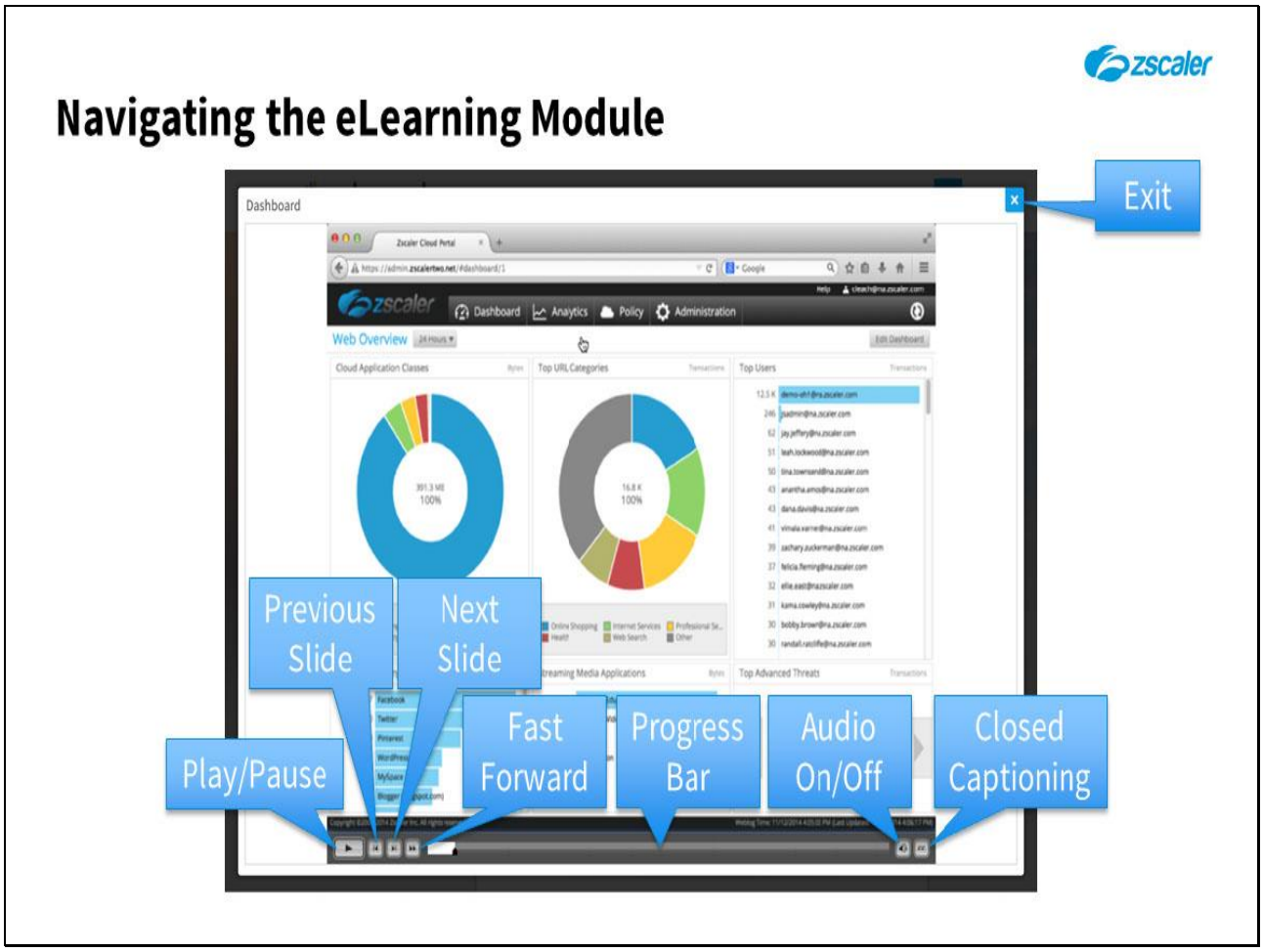
Slide 1 - Zscaler Policies



Slide notes

Welcome to the Zscaler Web ‘Security’ Policies Module.

Slide 2 - Navigating the eLearning Module



Slide notes

Here is a quick guide to navigating this module. There are various controls for playback including play and pause, previous, 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 at the top to exit.

Slide 3 - Agenda

Slide notes

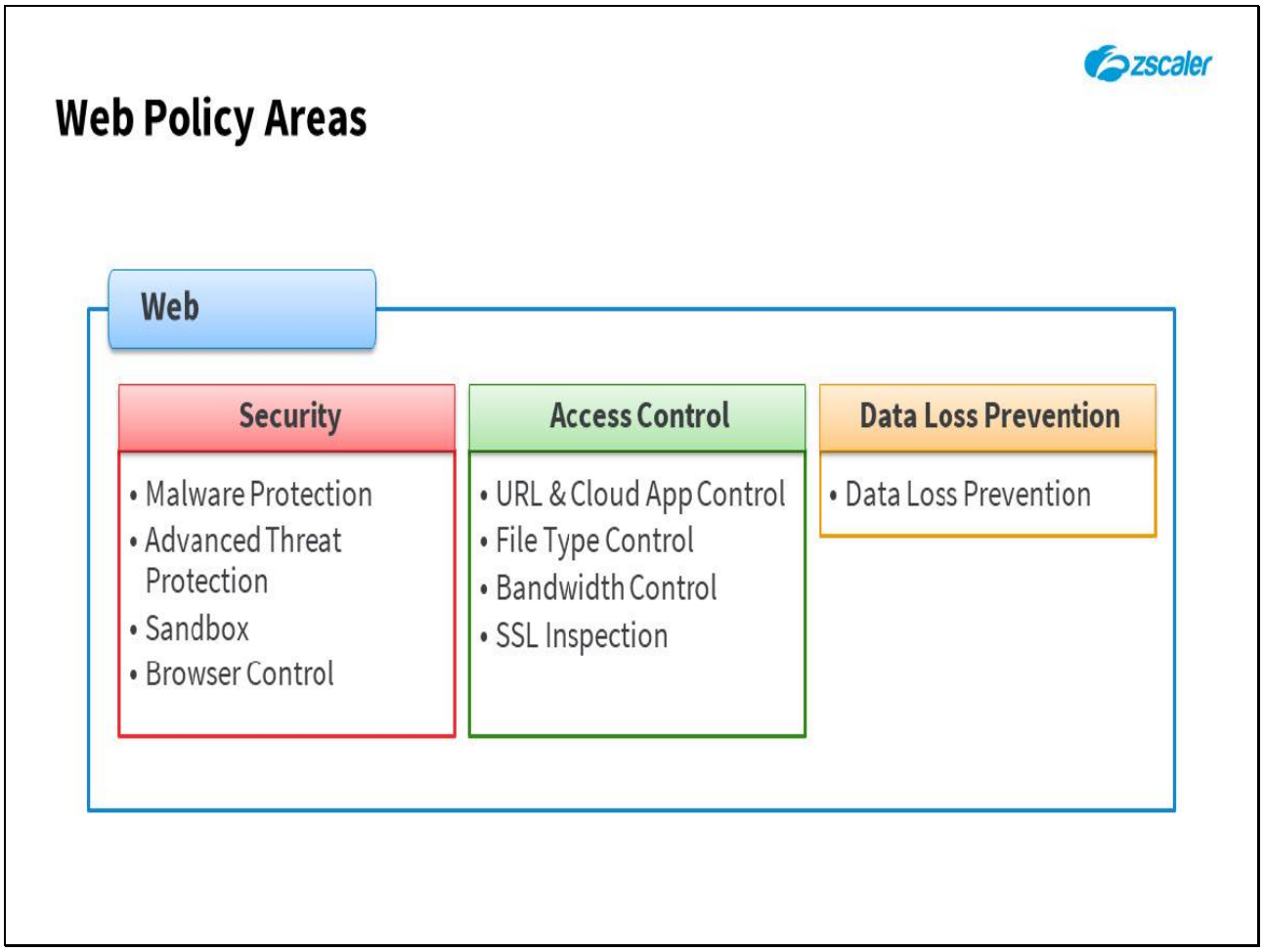
In this module, we will cover: an overview of the Web policies available; and a detailed look at the available Web 'Security' policies.

Slide 4 - Web Policy Overview

Slide notes

The first topic we will cover is an overview of the available Web policies.

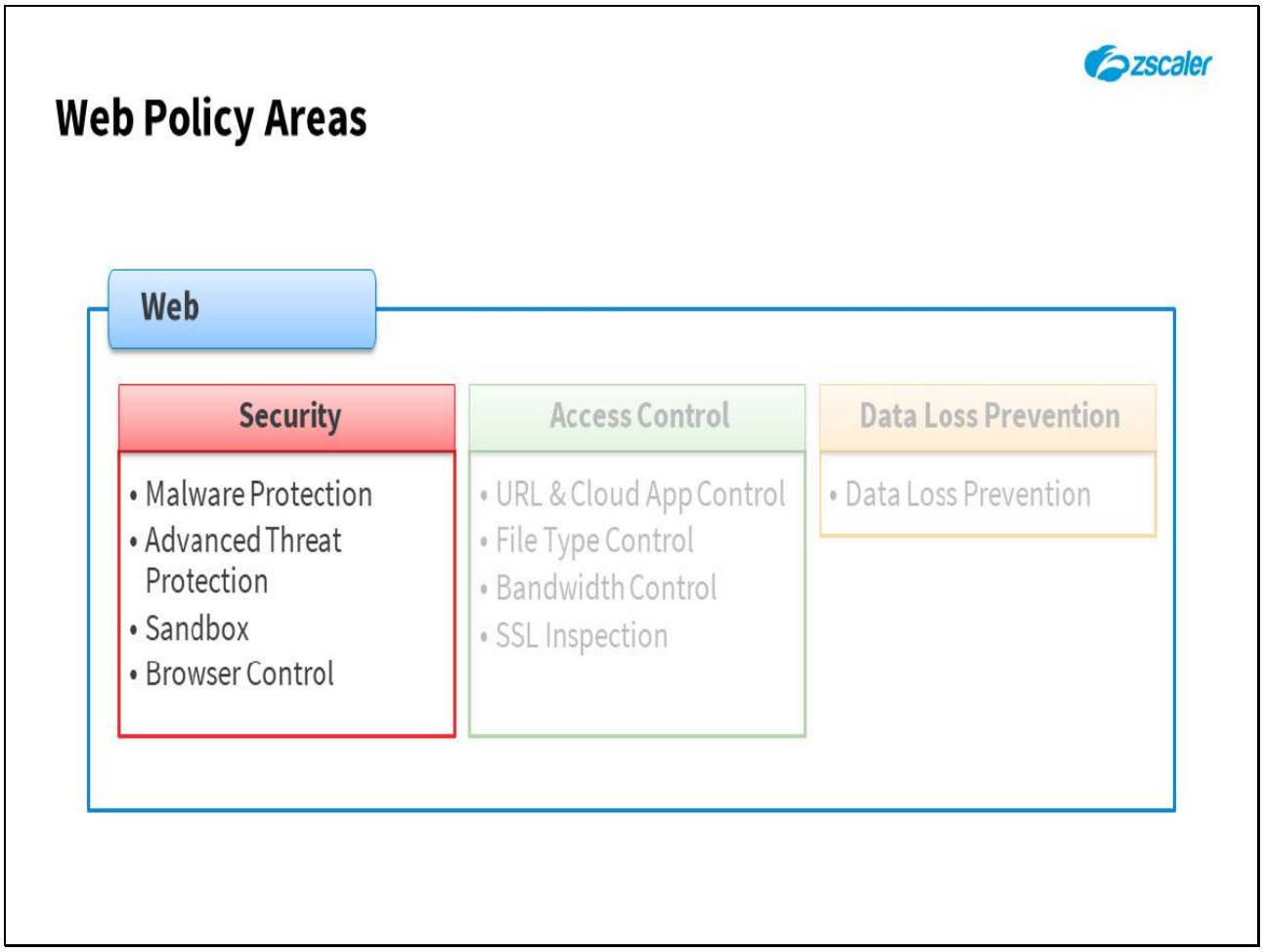
Slide 5 - Web Policy Areas



Slide notes

The Web policy area is the most extensive of the policy areas, and allows the creation of 'Security', 'Access Control' and 'Data Loss Prevention' policies.

Slide 6 - Web Policy Areas



Slide notes

In this module, we will look at each of the policies available in the 'Security' category and provide some recommendations for the policy settings.

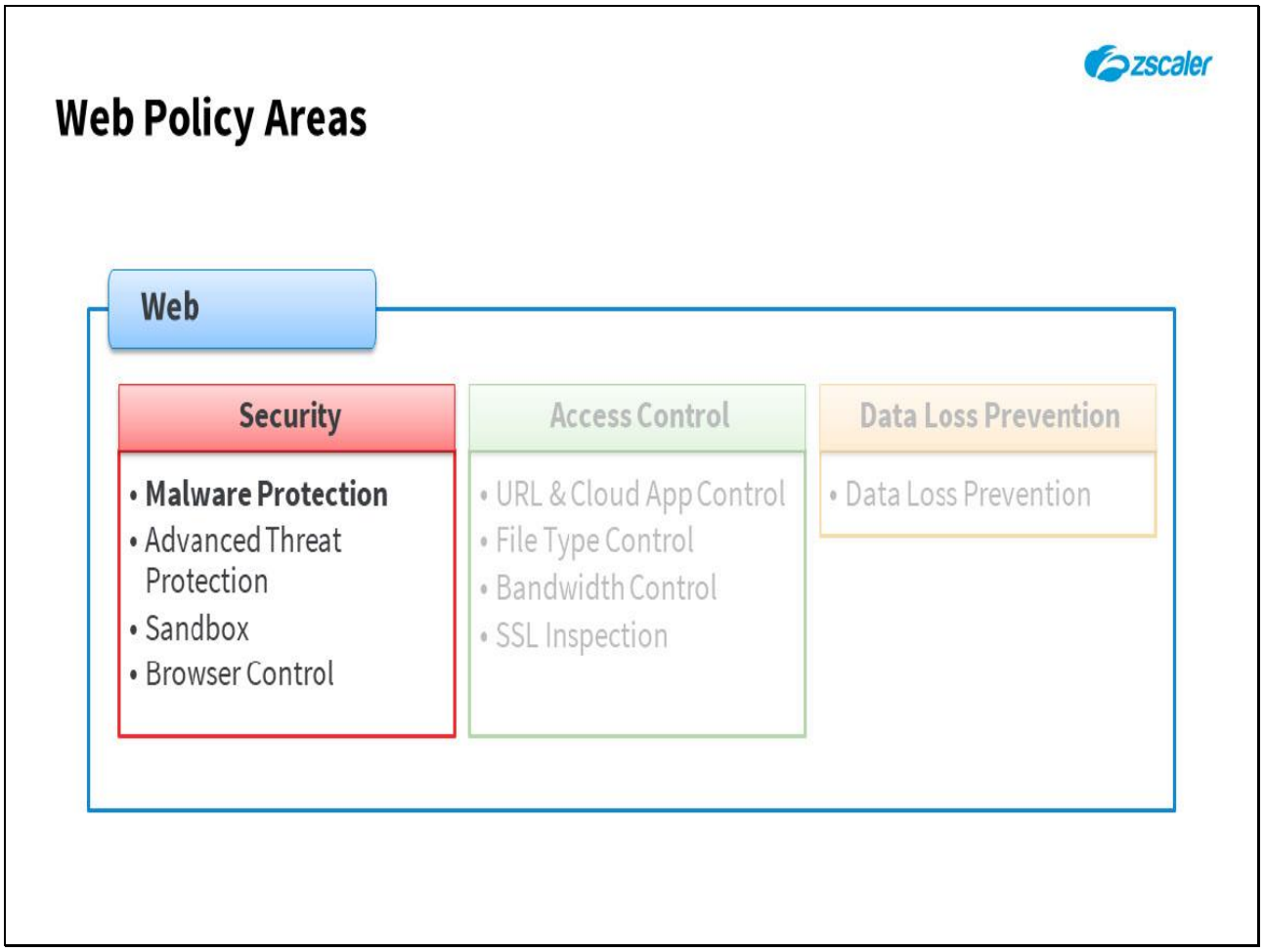
Slide 7 - Interactive Demo: Web Policy – Security

Slide notes

In the next section, we will have a detailed look at the Web 'Security' Policies.

This section has been created as an interactive demo to give you a feel for the navigation of the Zscaler Admin Portal UI. You will be asked to select the appropriate menu options to navigate the UI. You may also use the Play control to proceed to the next step.

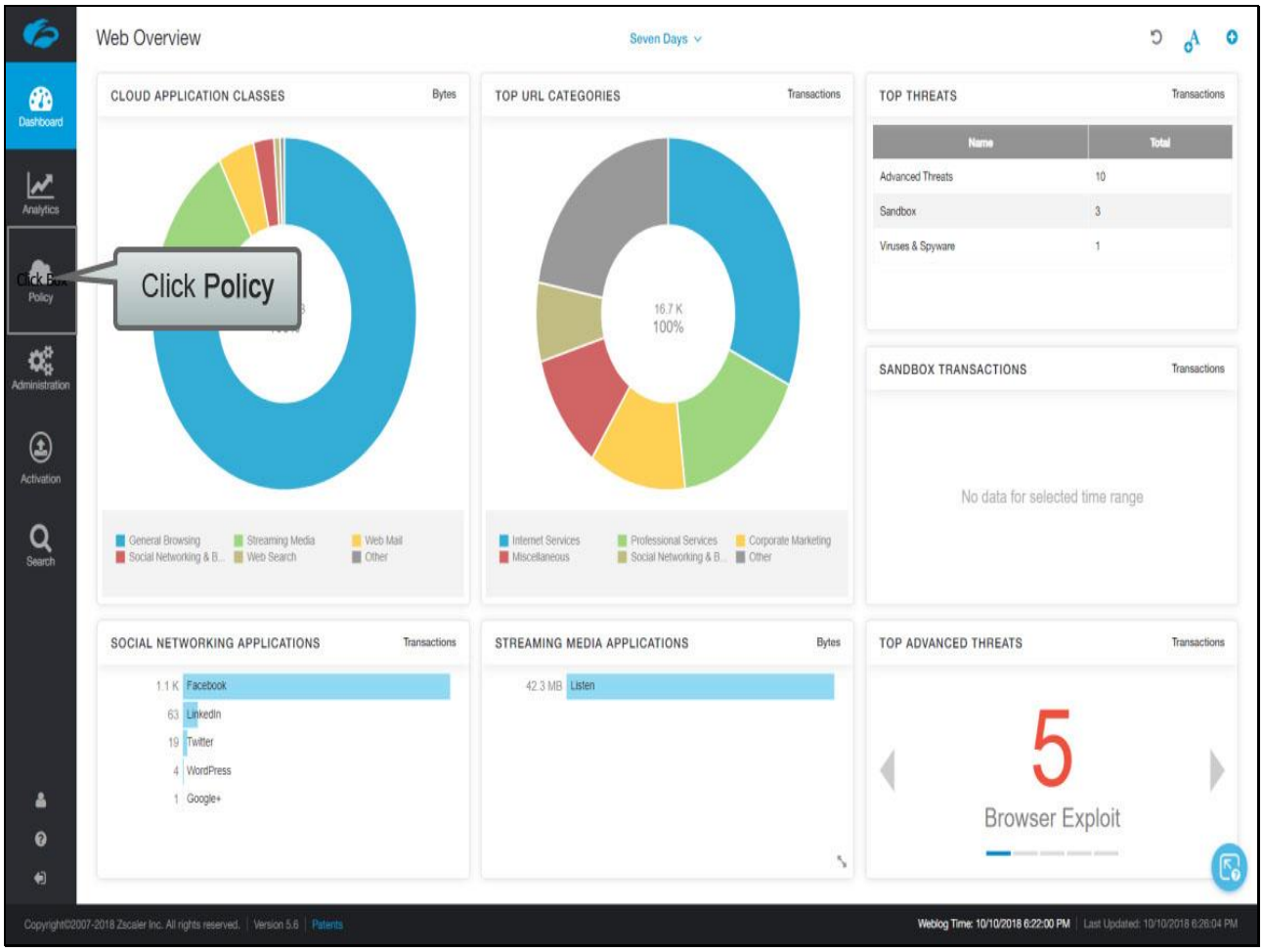
Slide 8 - Web Policy Areas



Slide notes

The first policy option that we will look at is 'Malware Protection'. This Policy protects your traffic against 'Malware', 'Adware', and 'Spyware'.

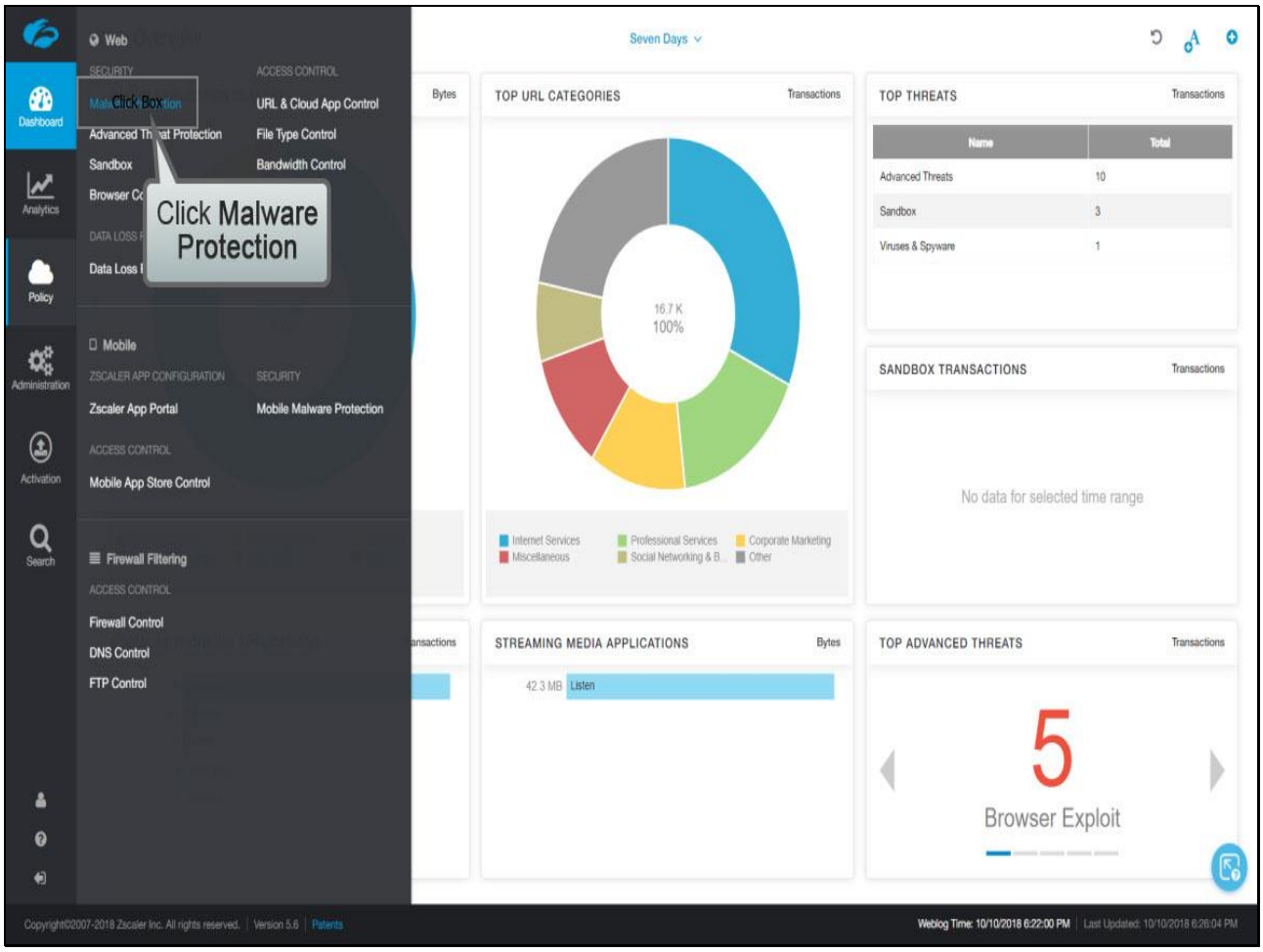
Slide 9 - Slide 9



Slide notes

To access the 'Malware Protection' policy settings, click 'Policy', …

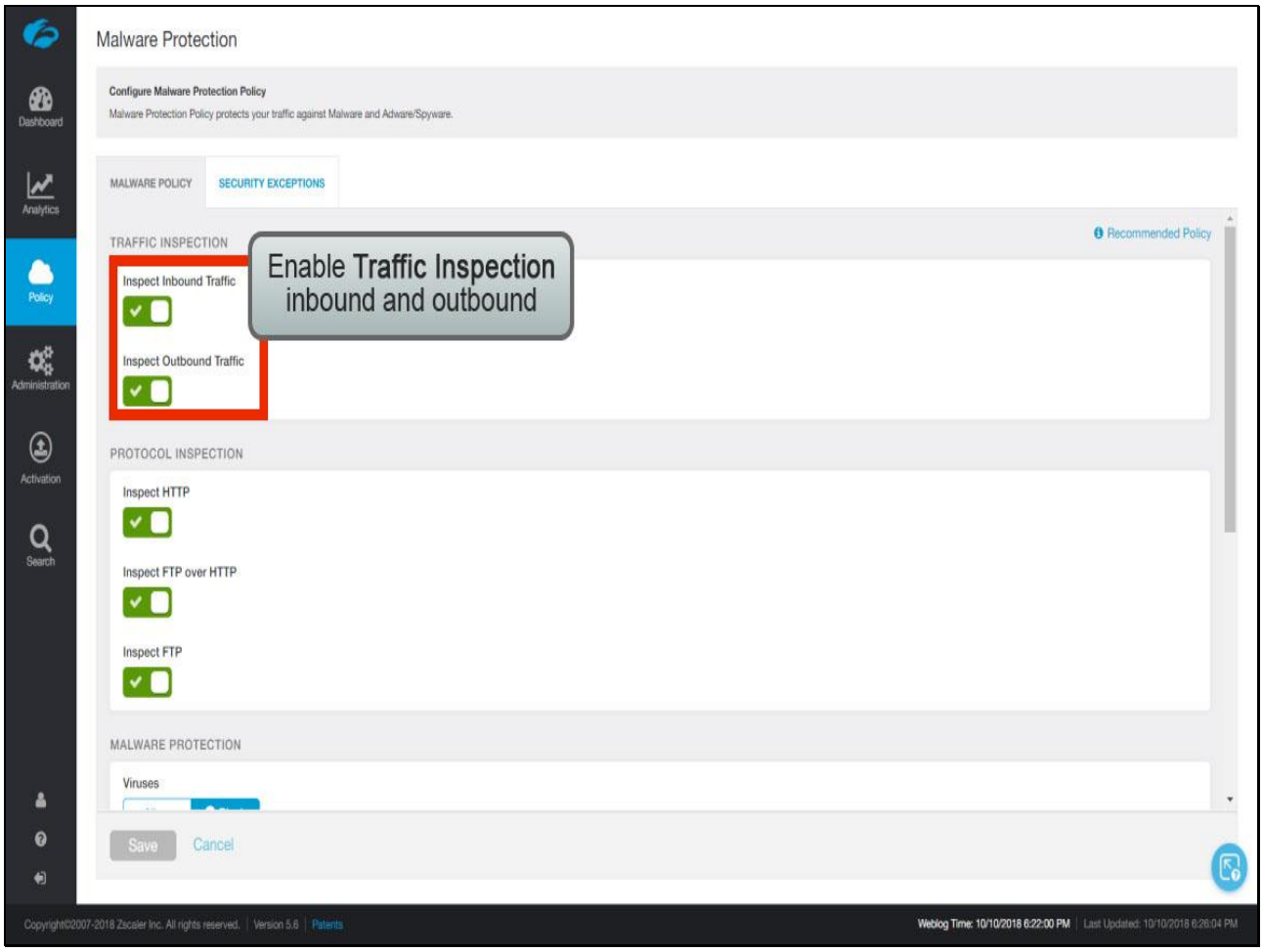
Slide 10 - Slide 10



Slide notes

…then from the ‘Web’ section of the ‘Policy’ menu, under the ‘SECURITY’ heading, click ‘Malware Protection’.

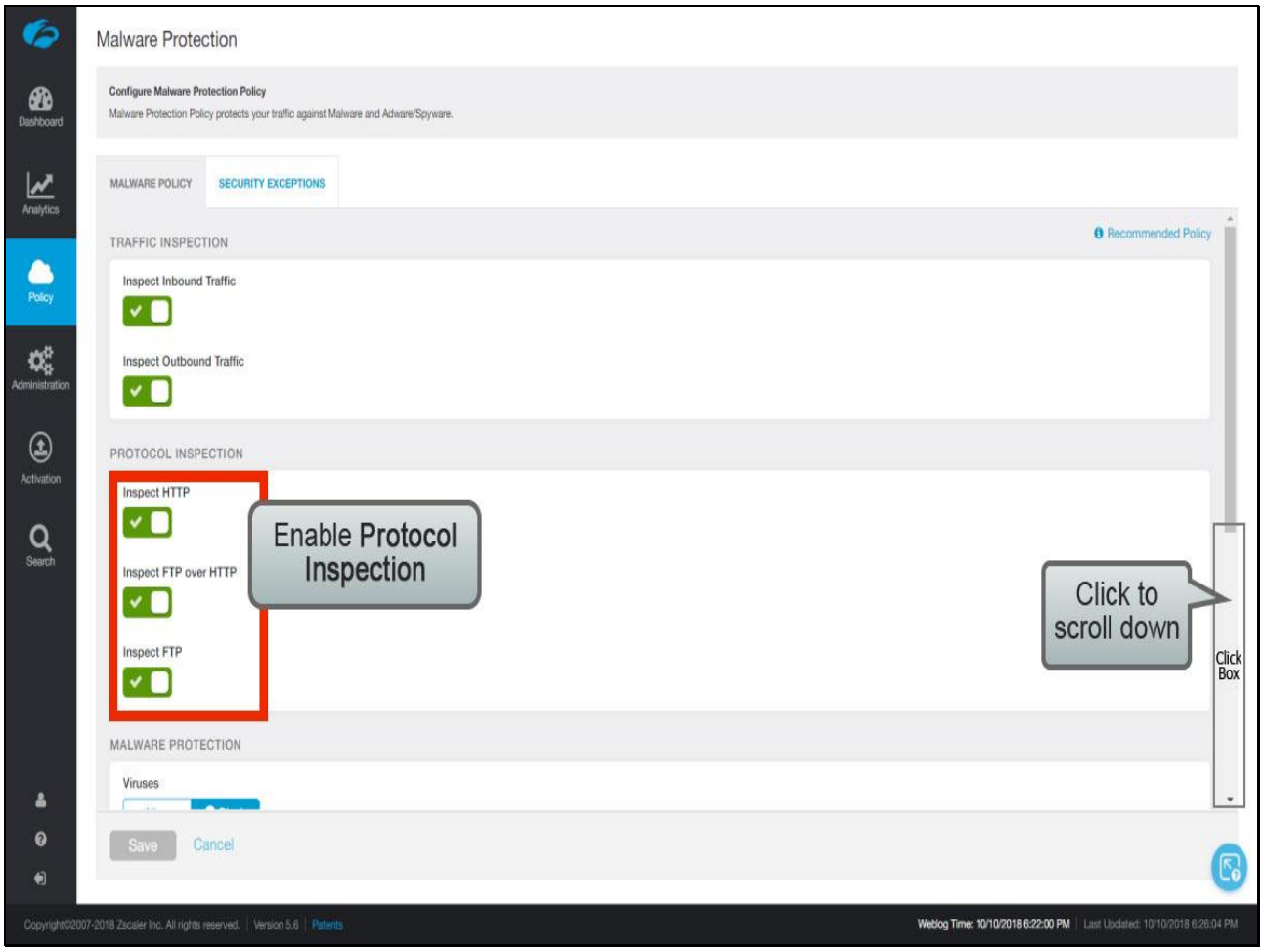
Slide 11 - Slide 11



Slide notes

The first section on the 'MALWARE POLICY' tab controls whether Zscaler inspects your traffic for Malware, and scanning is enabled by default for both outbound, and return traffic. If you disable these options, then Zscaler will not inspect your traffic for Malware at all.

Slide 12 - Slide 12

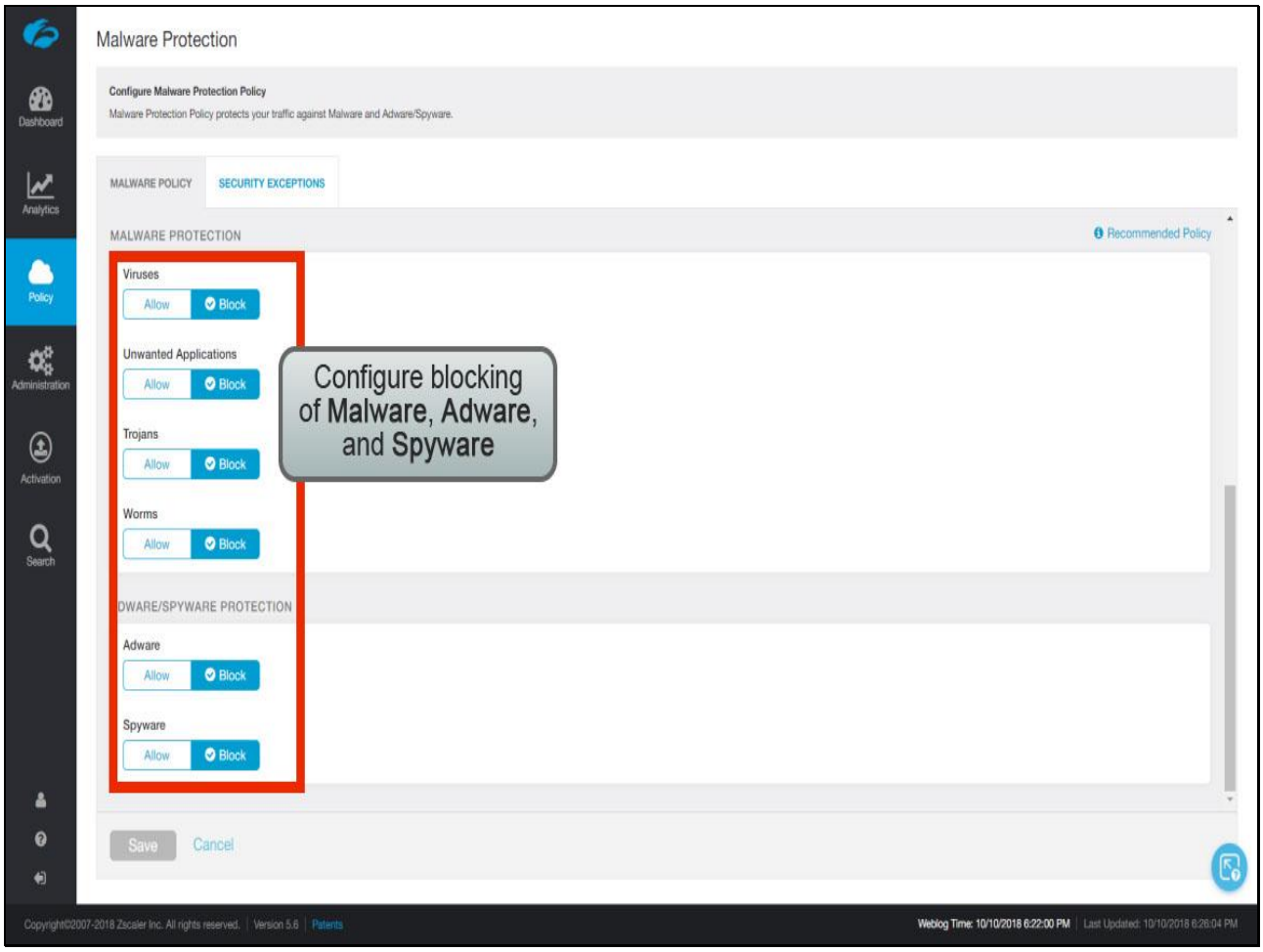


Slide notes

In the next section, you can specify which protocols to scan for Malware, the options being HTTP, FTP over HTTP, and native FTP. Note that this is a global setting, and also controls whether traffic is scanned for the Anti-Virus, Anti-Malware, Anti-Spyware, Advanced Threat Protection, and Sandbox policies.

Click to scroll to the bottom of this page.

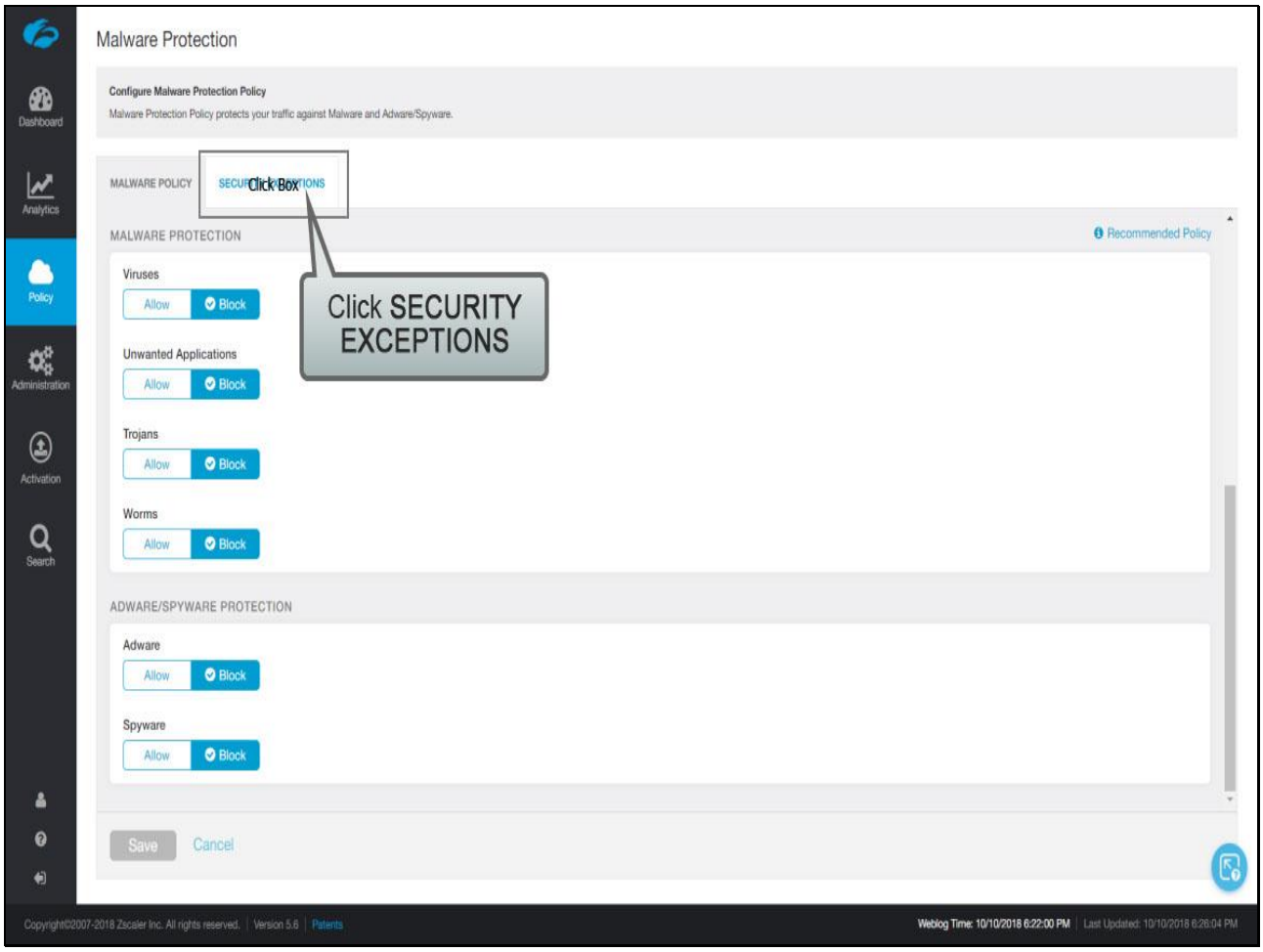
Slide 13 - Slide 13



Slide notes

The other sections on this page allow you to allow or block various types of ‘Malware’, ‘Adware’, and ‘Spyware’, and by default all of these are enabled.

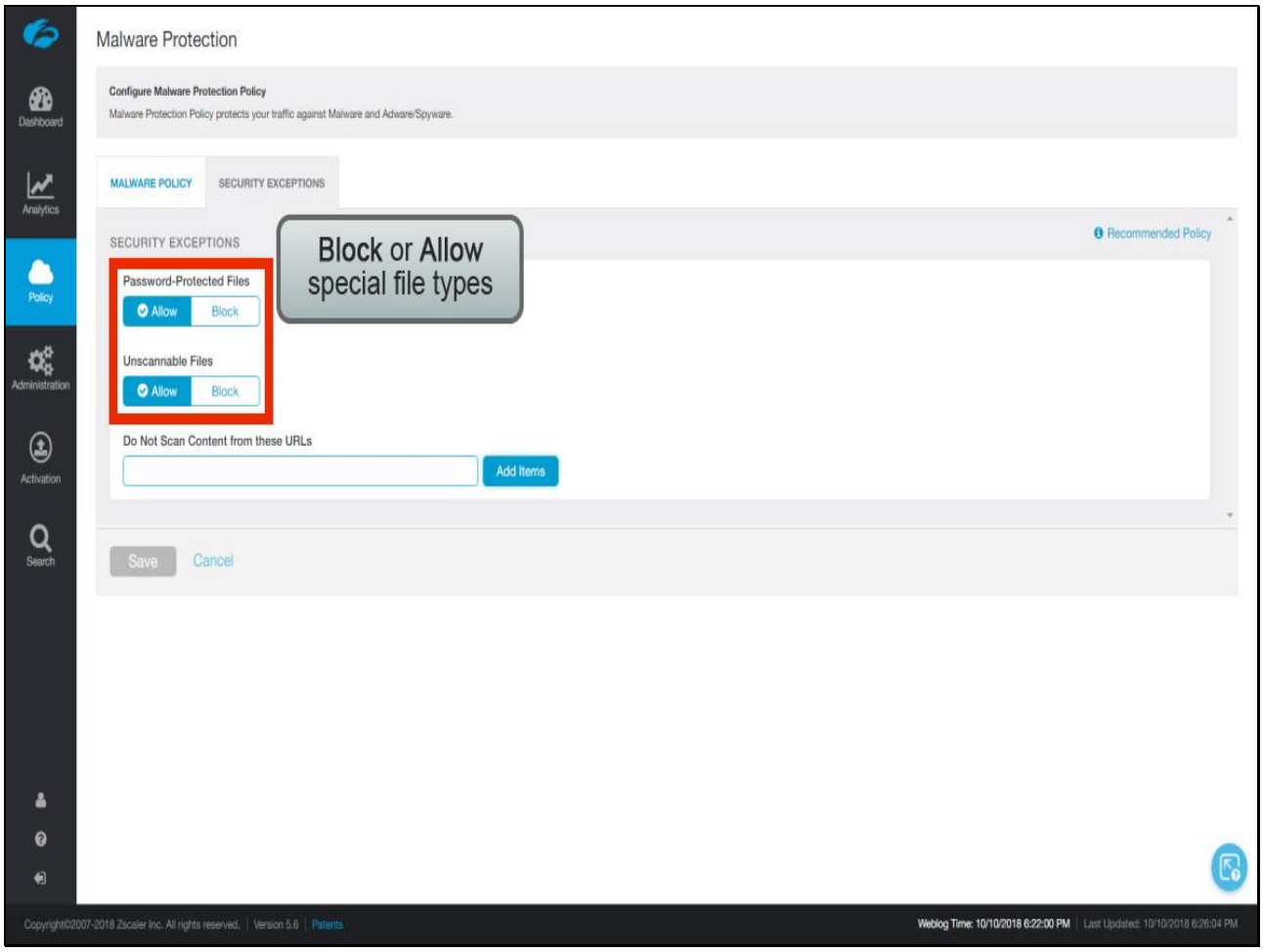
Slide 14 - Slide 14



Slide notes

It is possible to configure exceptions to the 'Malware Protection' Policy, and this is done by clicking on the 'SECURITY EXCEPTIONS' tab.

Slide 15 - Slide 15

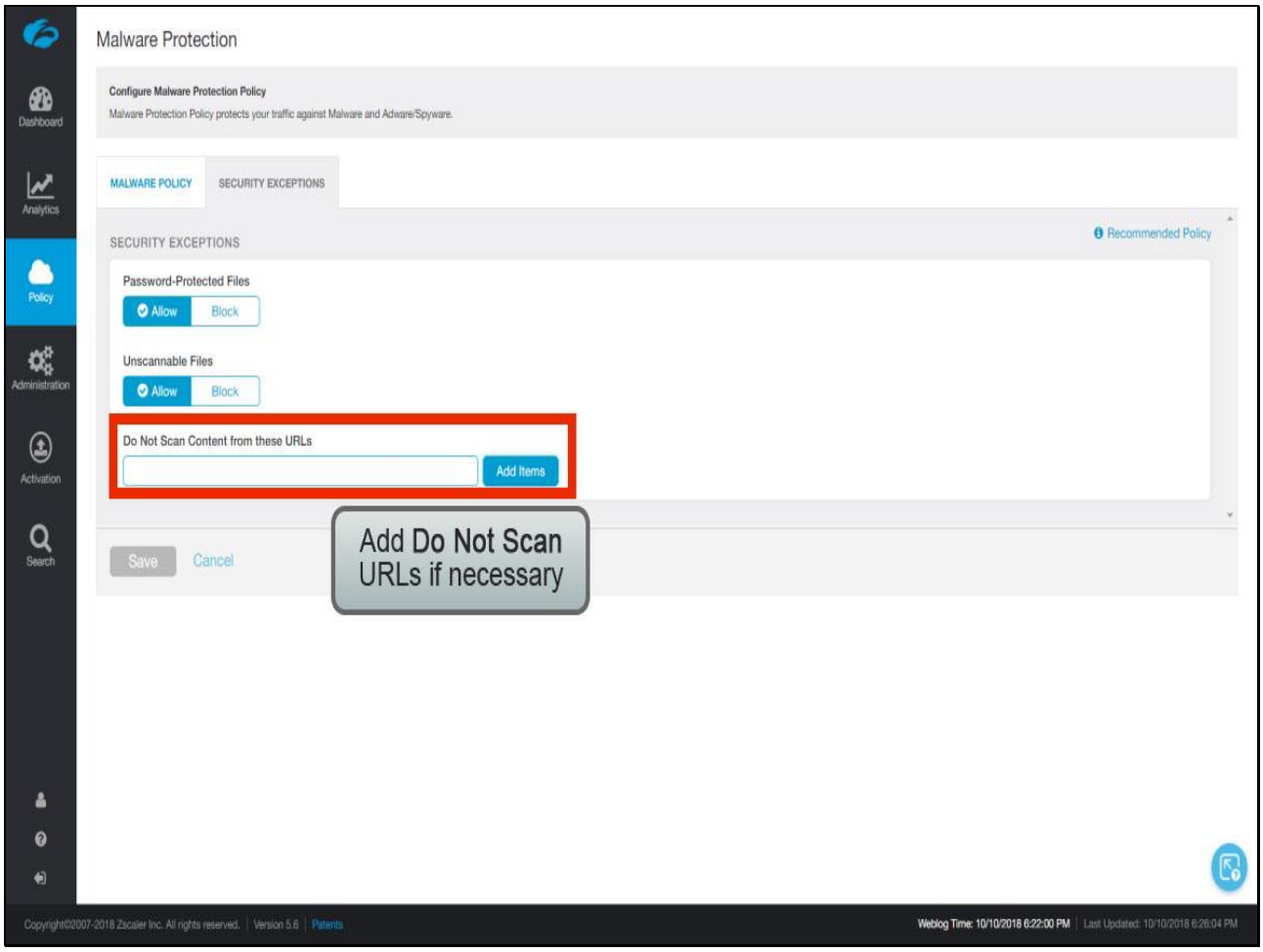


Slide notes

Password protected .ZIP and .RAR files are allowed by default, but you can click 'Block' to stop users from uploading or downloading these types of file. In addition, 'Unscannable Files' are allowed by default, and you also have the option to block them.

Zscaler may not be able to scan some files due to an unrecognized file format, excessive size, or recursive compression. If you elect to block users from downloading or uploading unscannable files, Zscaler will notify the user that the password-protected or unknown file could not be scanned by the AV application, and that the entire transaction has failed.

Slide 16 - Slide 16

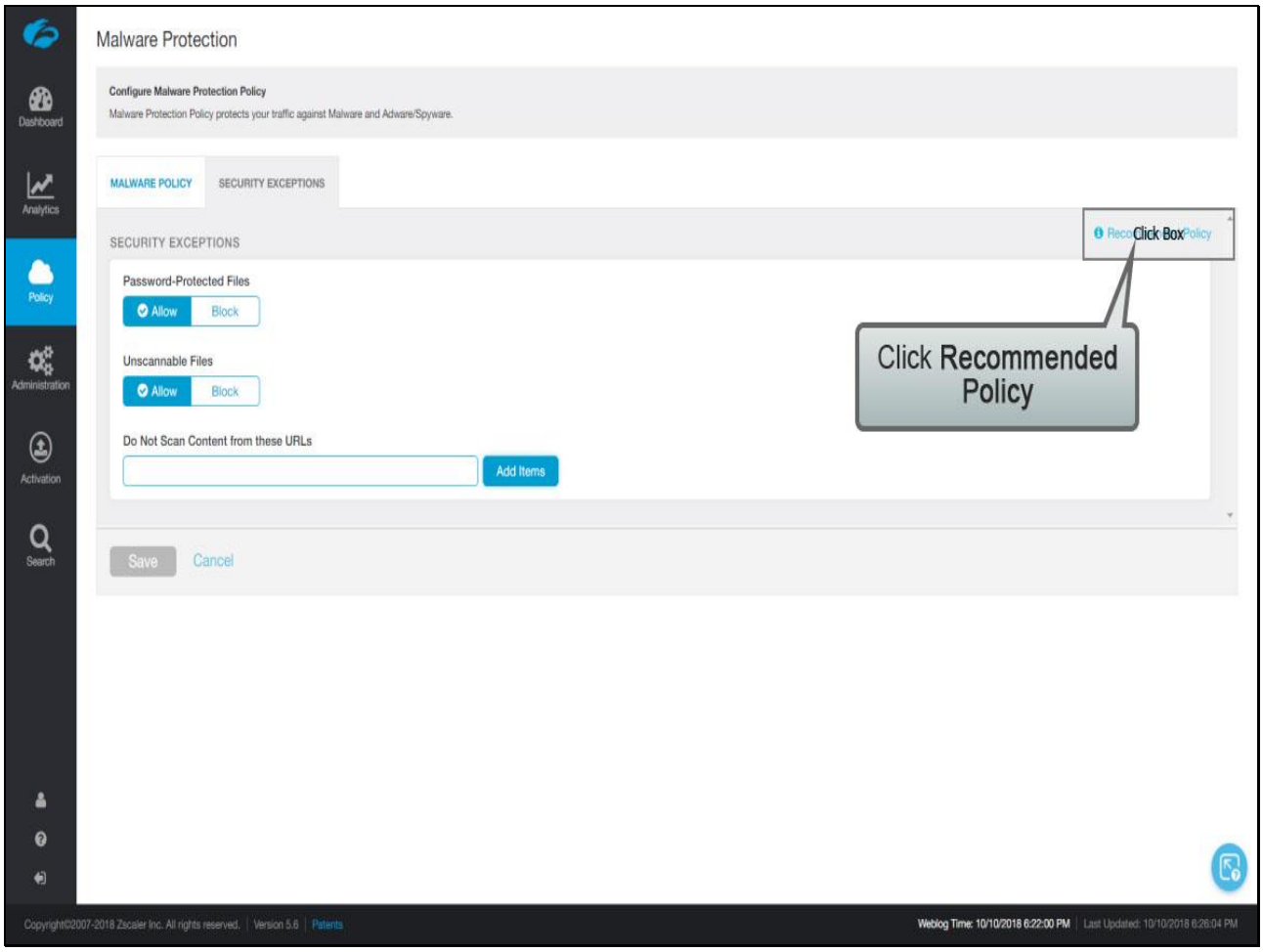


Slide notes

There may be trusted Web sites of partners or vendors, whose webmail or file downloads might otherwise be blocked due to anti-virus, anti-spyware, or anti-malware policies. You can exempt these sites from inspection by adding them to the 'Do Not Scan Content from these URLs' list. Zscaler will allow users to download content from the URLs added here without inspecting the traffic.

Note that this is a global list, and traffic from any of the sites listed here will also bypass anti-virus, anti-malware, anti-spyware, 'Advanced Threat Protection', and 'Sandbox' checks. The syntax for adding URLs here is discussed in the 'Policy Fundamentals' module.

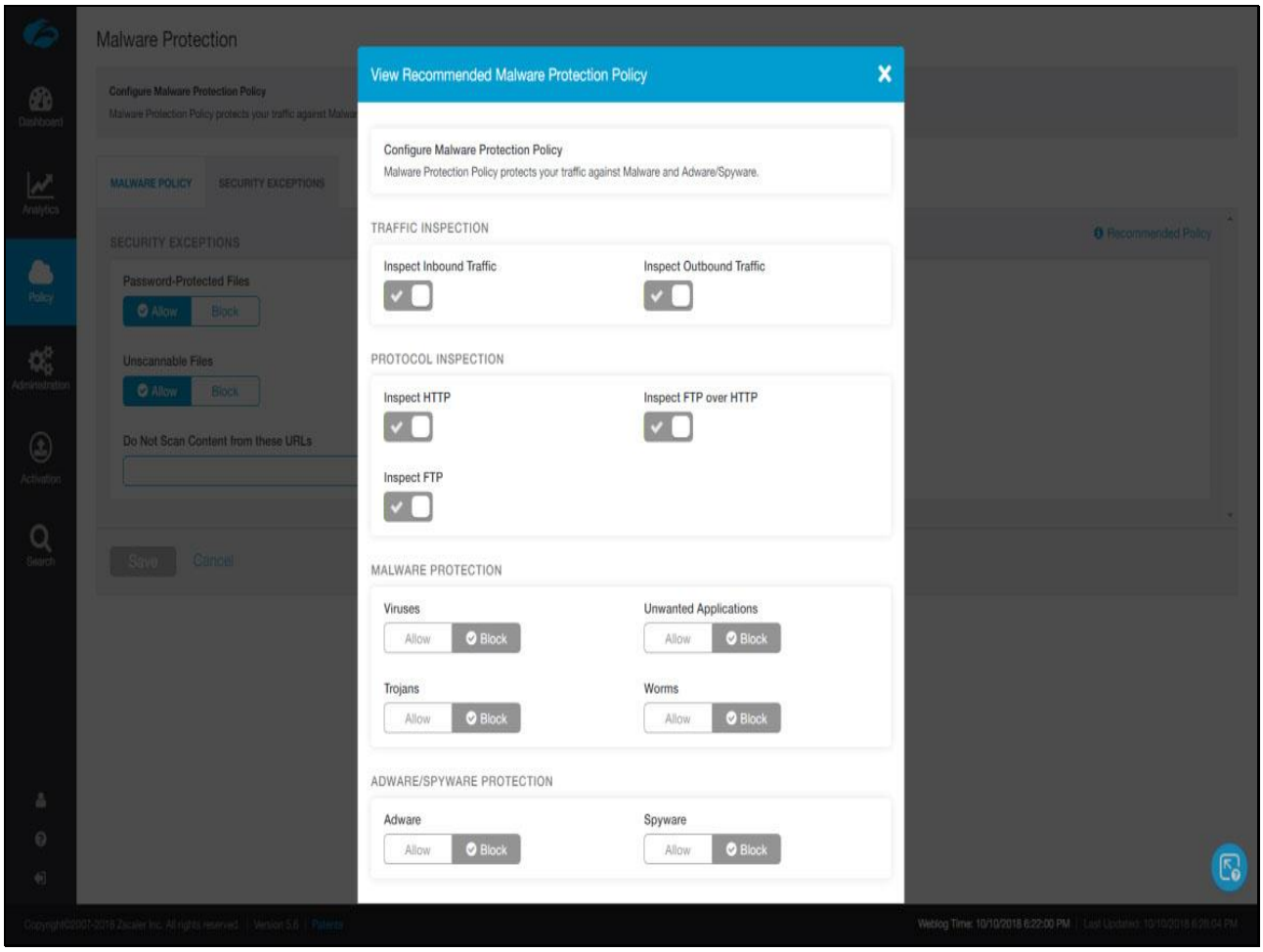
Slide 17 - Slide 17



Slide notes

To view Zscaler recommendations for configuring ‘Malware Protection’ Policy settings, click the ‘Recommended Policy’ link.

Slide 18 - Slide 18



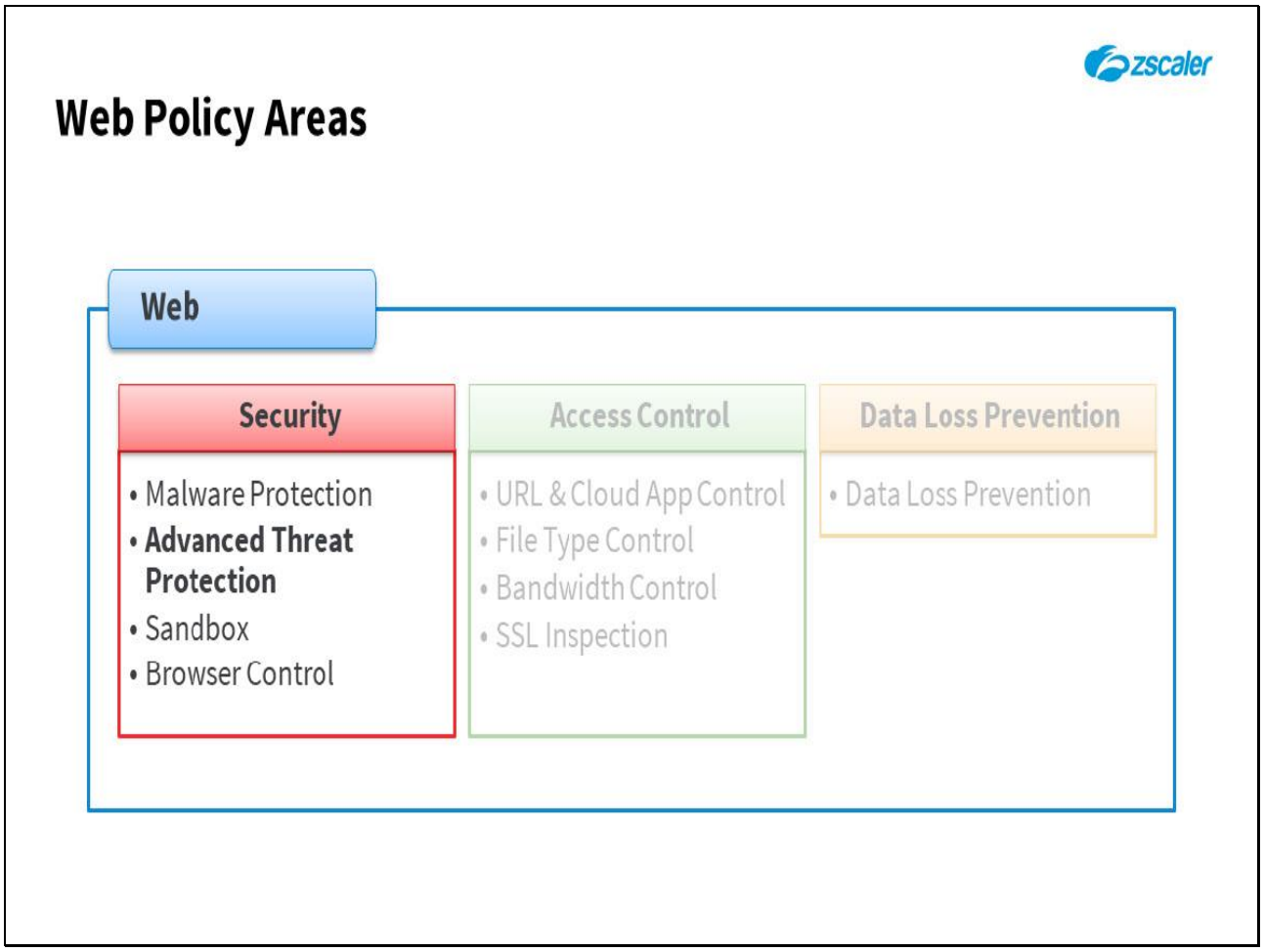
Slide notes

The 'Malware Protection' Policy applies globally to all of your locations, and the recommended configuration is to:

- Enable 'Traffic Inspection' in both directions, and 'Protocol Inspection' for all protocols;
- To set all 'Malware', 'Adware', and 'Spyware' types to 'Block'; with no 'Security Exceptions'.

Be sure to 'Save' and 'Activate' any changes you make to the Policy.

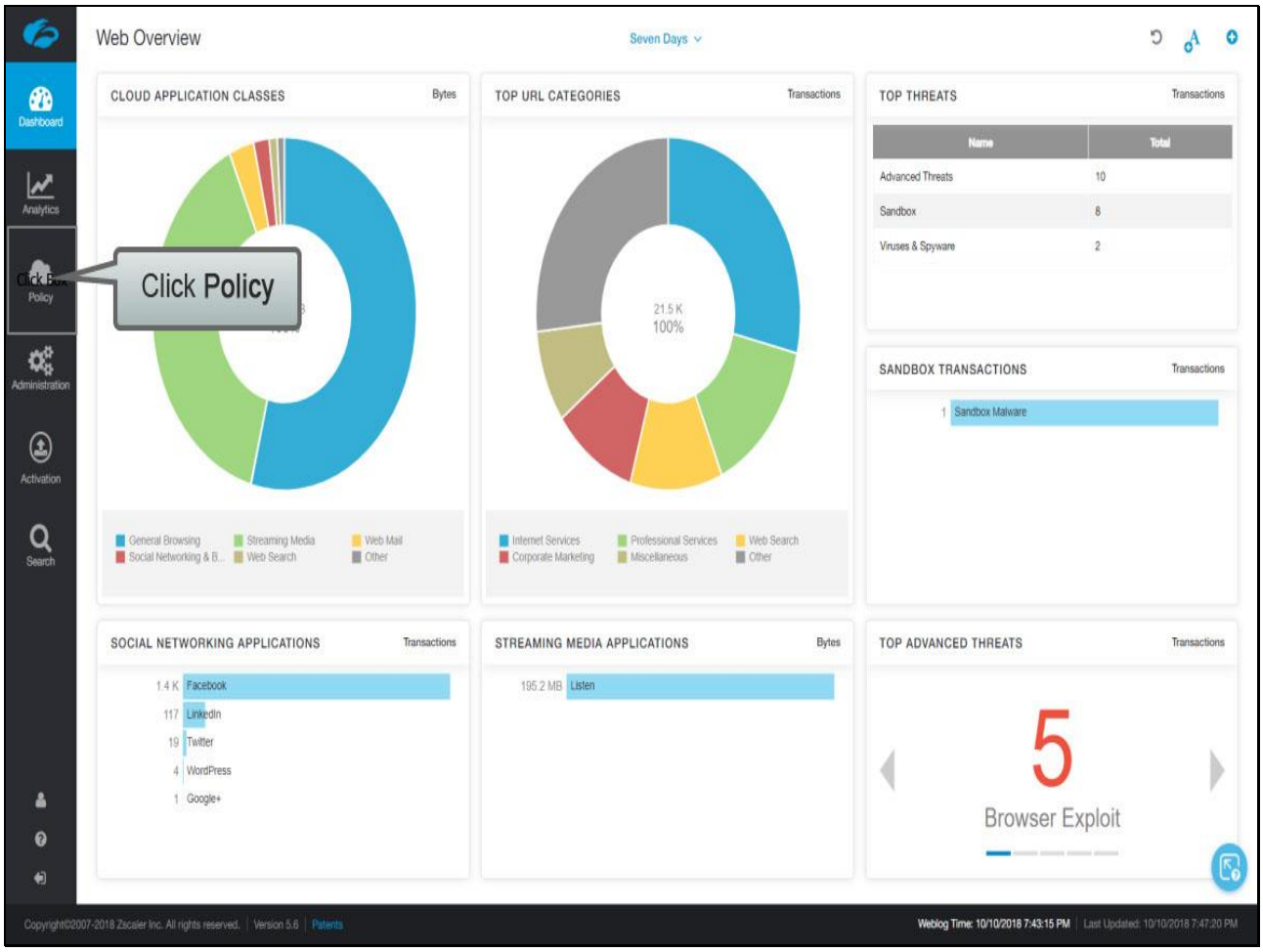
Slide 19 - Web Policy Areas



Slide notes

The 'Advanced Threat Protection' Policy protects your traffic against 'Botnets', 'Malicious Active Content', 'Fraud', 'Unauthorized Communication', 'Cross-Site Scripting (XSS)', 'Suspicious Destinations', and 'Peer-to-Peer (P2P) File Sharing'.

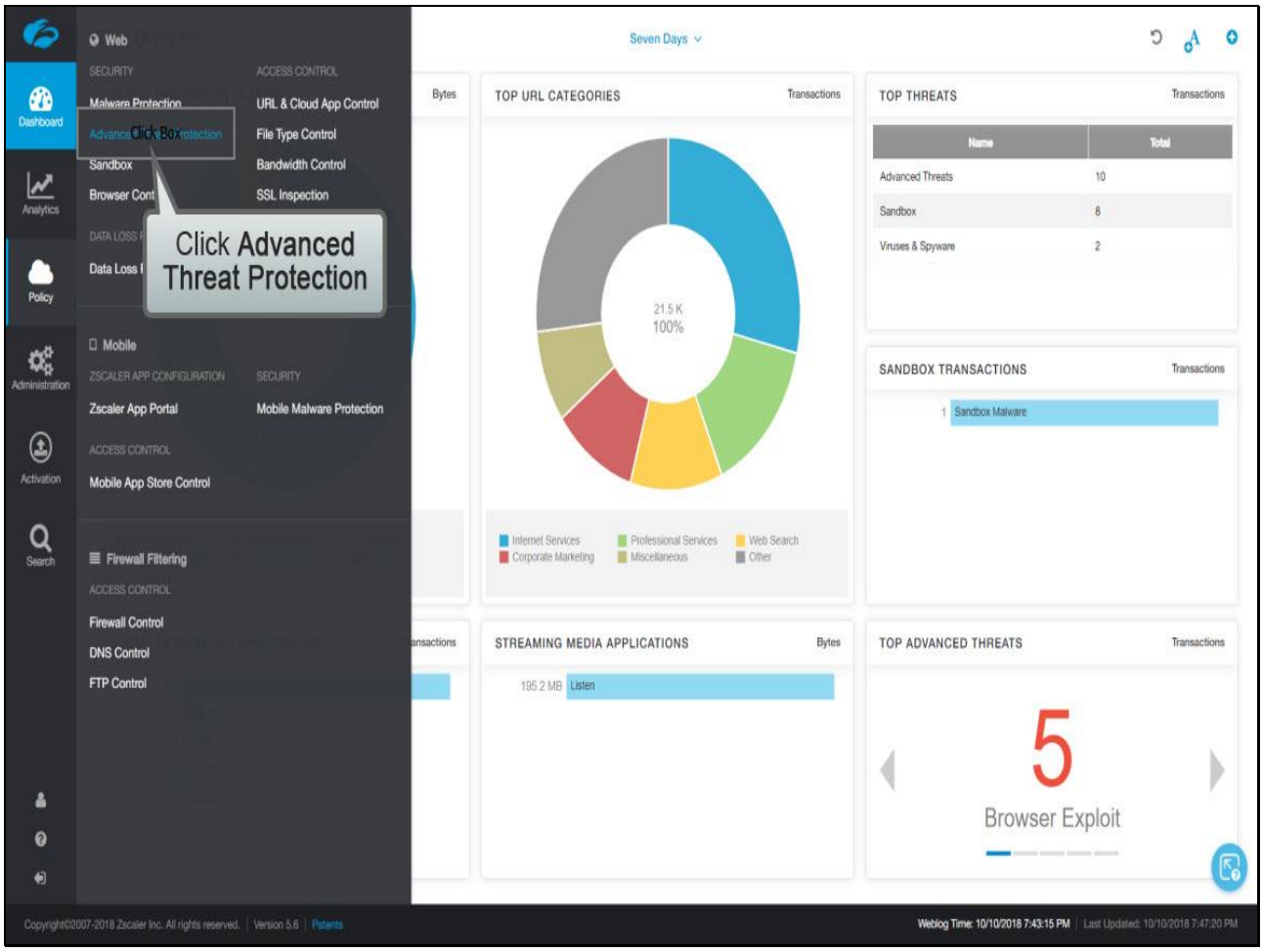
Slide 20 - Slide 20



Slide notes

To access the 'Advanced Threat Protection' policy settings, click 'Policy', …

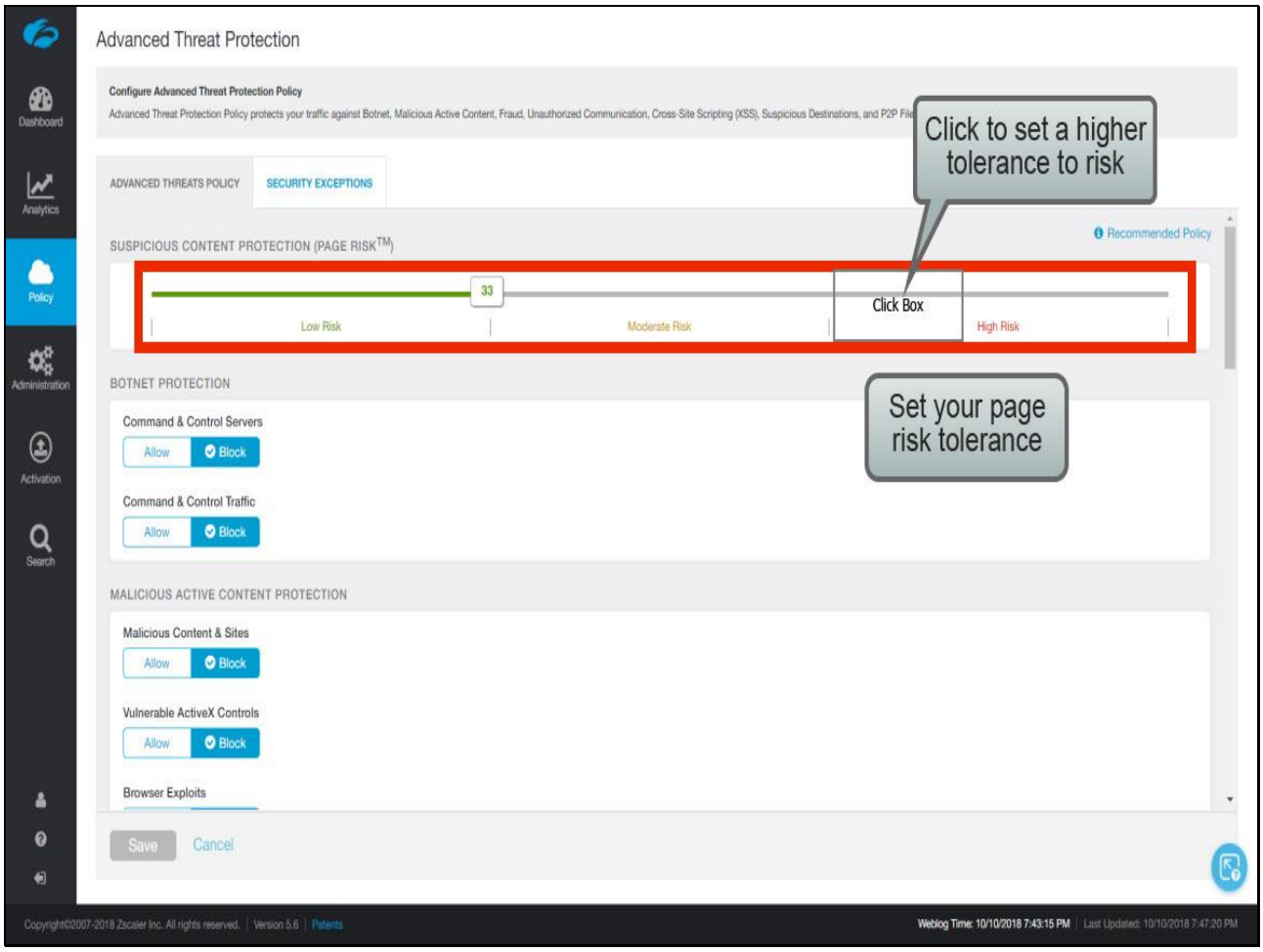
Slide 21 - Slide 21



Slide notes

…then from the ‘Web’ section of the ‘Policy’ menu, under the ‘SECURITY’ heading, click ‘Advanced Threat Protection’.

Slide 22 - Slide 22



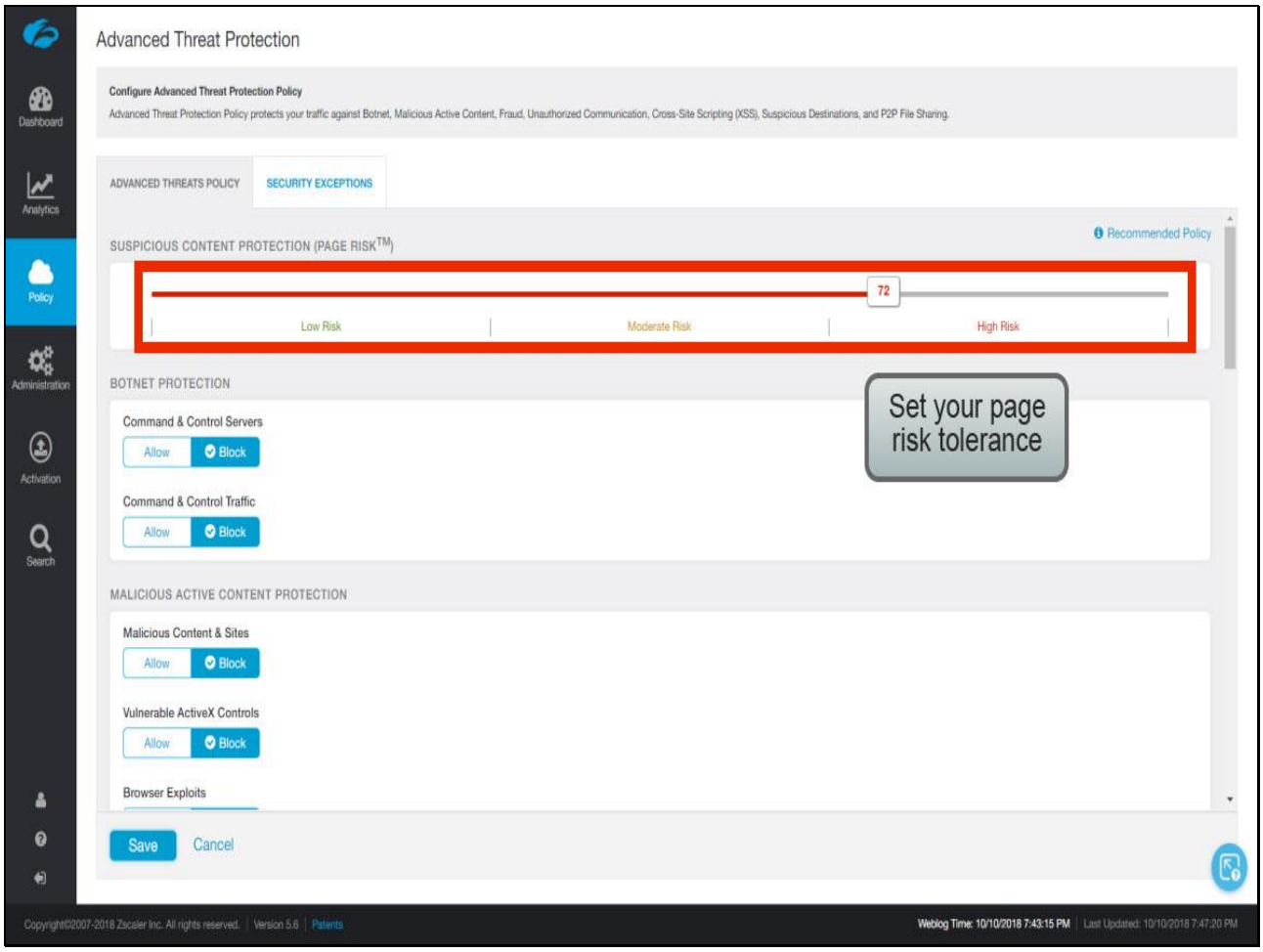
Slide notes

The 'ADVANCED THREATS POLICY' tab is broken into two main parts; the 'Suspicious Content Protection (PageRisk™)' slider at the top, and the options below it. Note that the page risk tolerance slider is independent of the 'Block'/'Allow' settings below it.

Zscaler calculates the 'Risk Index' of a page in real-time by identifying malicious content within the page, such as; injected scripts, vulnerable ActiveX, zero-pixel iFrames, and so on. Simultaneously, Zscaler creates a 'Domain Risk Index' using data such as; hosting country, domain age, past results, and links to high-risk top-level domains. The 'Page Risk' and 'Domain Risk' scores are combined to produce a single Risk Index.

This score is then compared to the page risk tolerance value that you set in this policy. Any sites with a 'Risk Index' greater than the page risk tolerance index will be blocked. Click on the slider to set your preferred tolerance to risk.

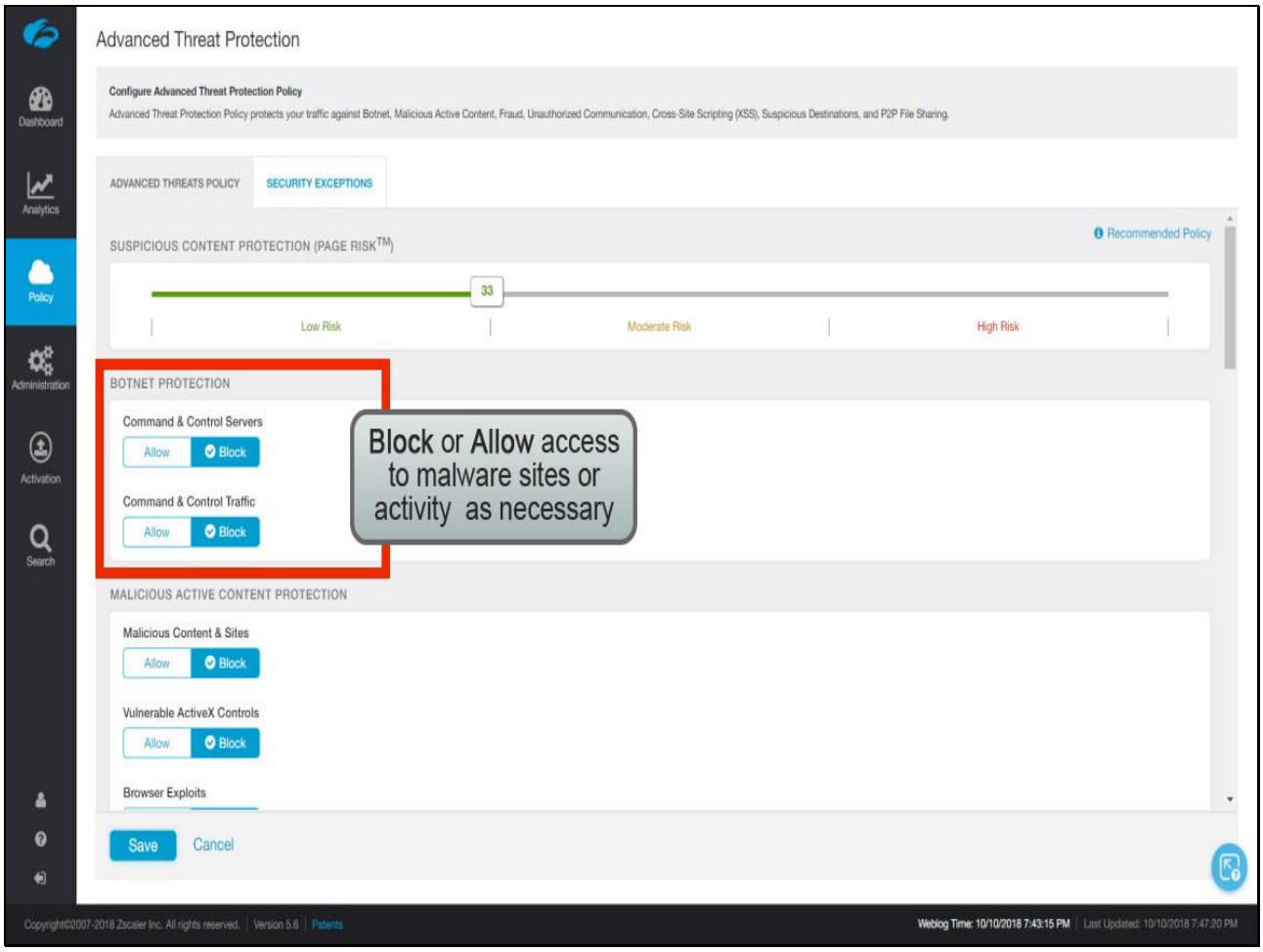
Slide 23 - Slide 23



Slide notes

So to reiterate, the further you move this slider to the right, the more risk you are willing to accept. By default, the page risk tolerance is set to 33.

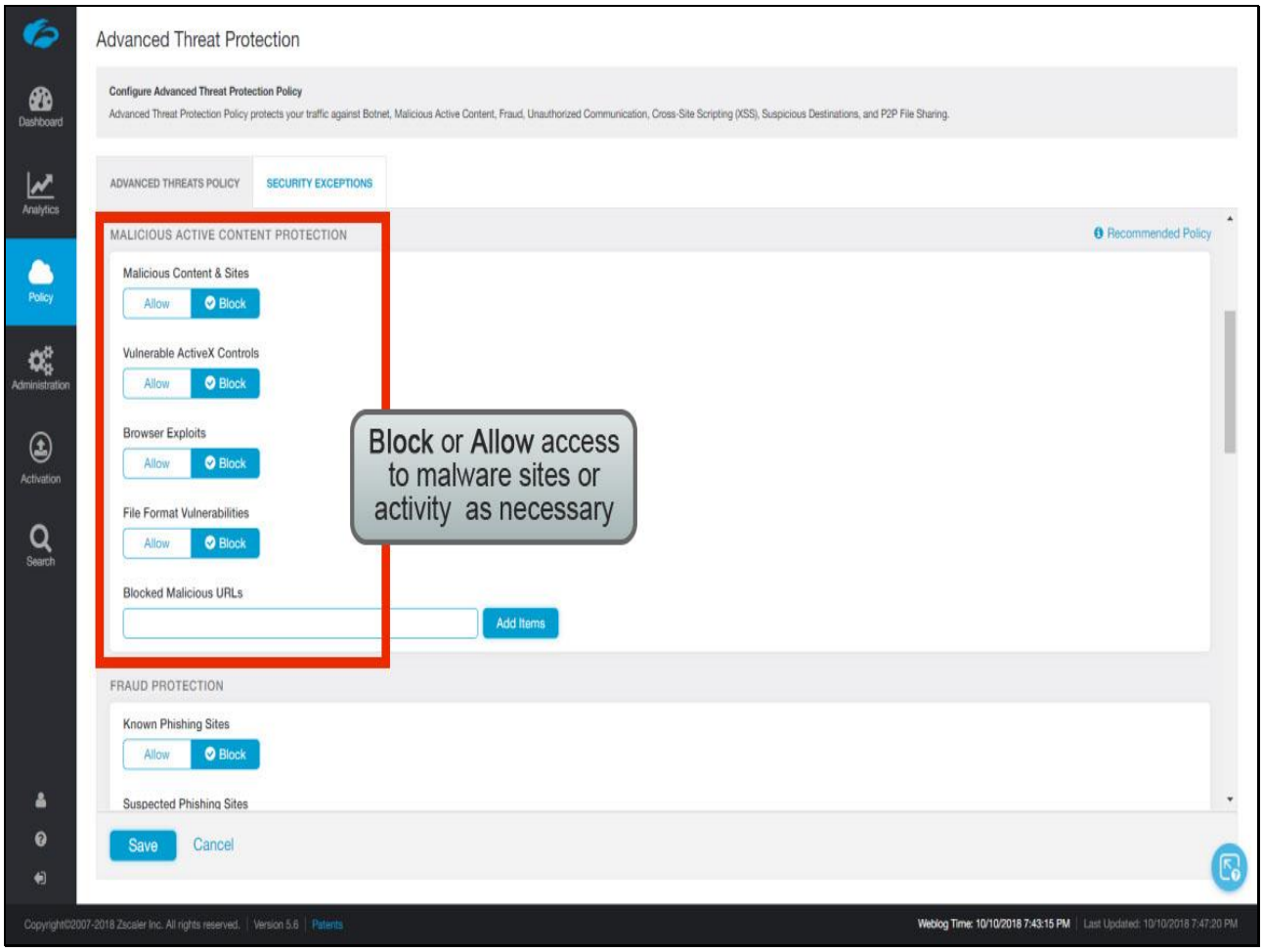
Slide 24 - Slide 24



Slide notes

The rest of the page contains ‘Block’ or ‘Allow’ controls for: ‘BOTNET PROTECTION’, …

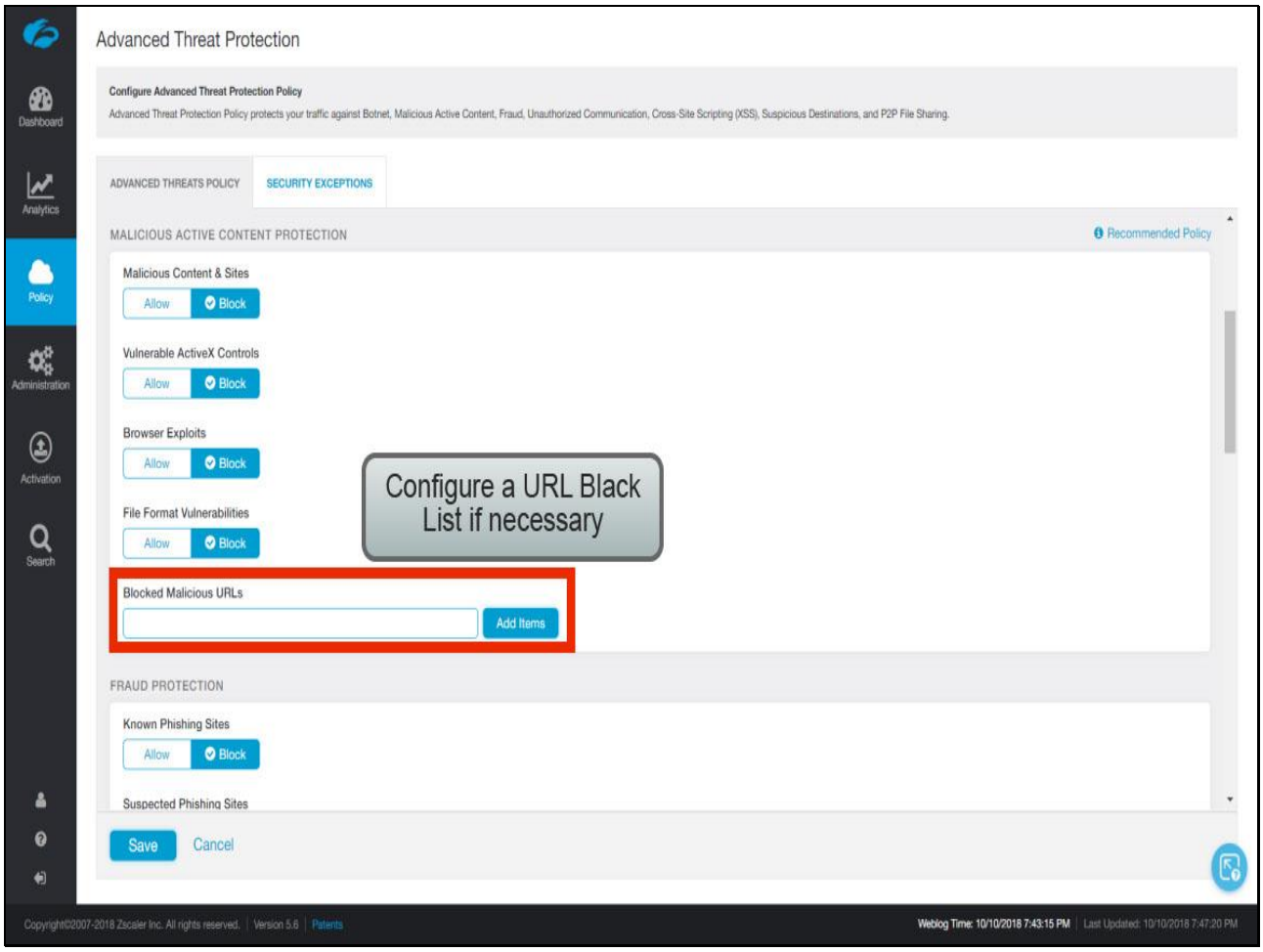
Slide 25 - Slide 25



Slide notes

…'MALICIOUS ACTIVE CONTENT PROTECTION', …

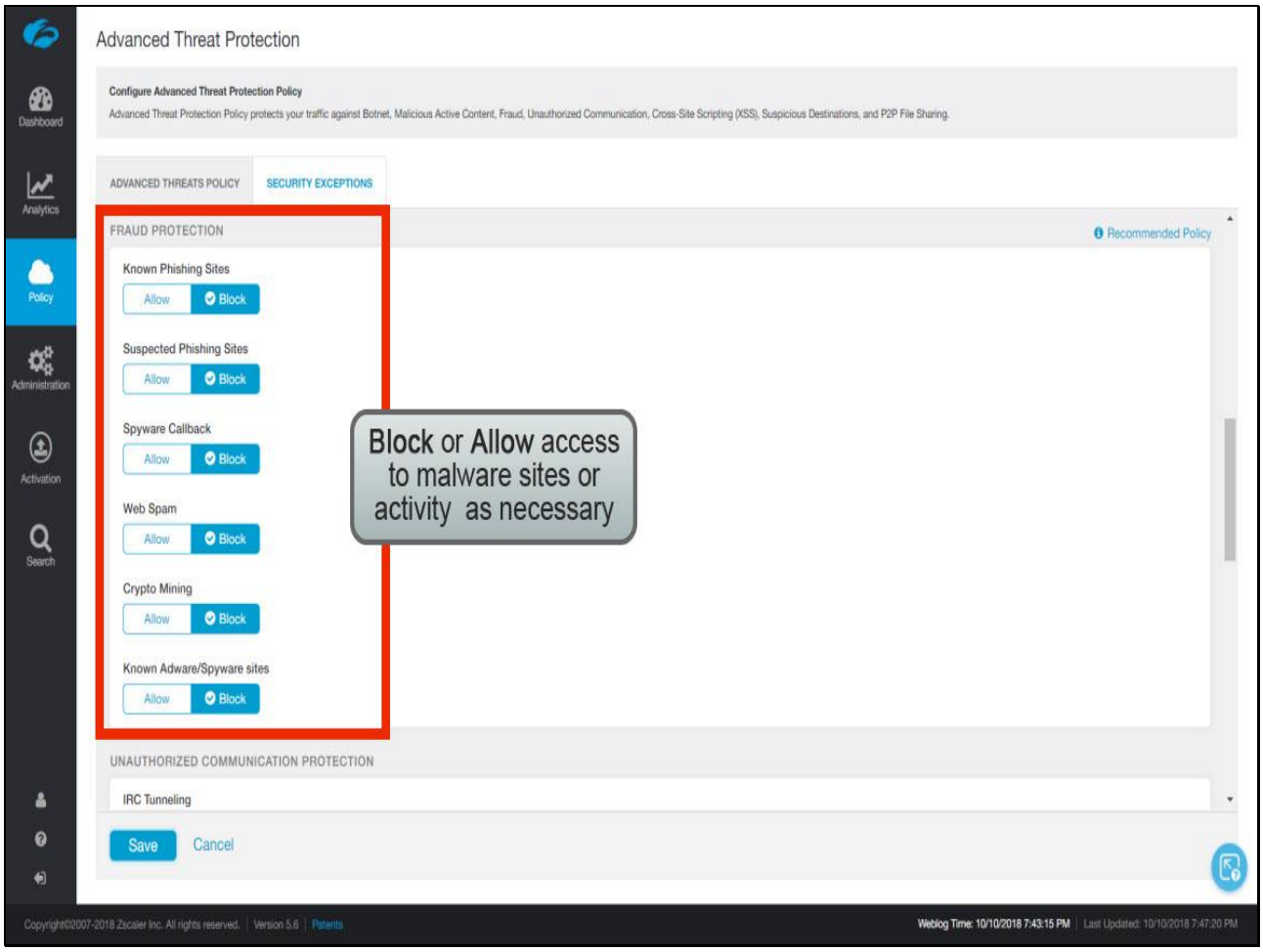
Slide 26 - Slide 26



Slide notes

…where it is also possible to set up a 'URL Black List'. Add any sites that you explicitly wish to block to the 'Blocked Malicious URLs' field. The syntax for adding URLs here is described in the 'Policy Fundamentals' module.

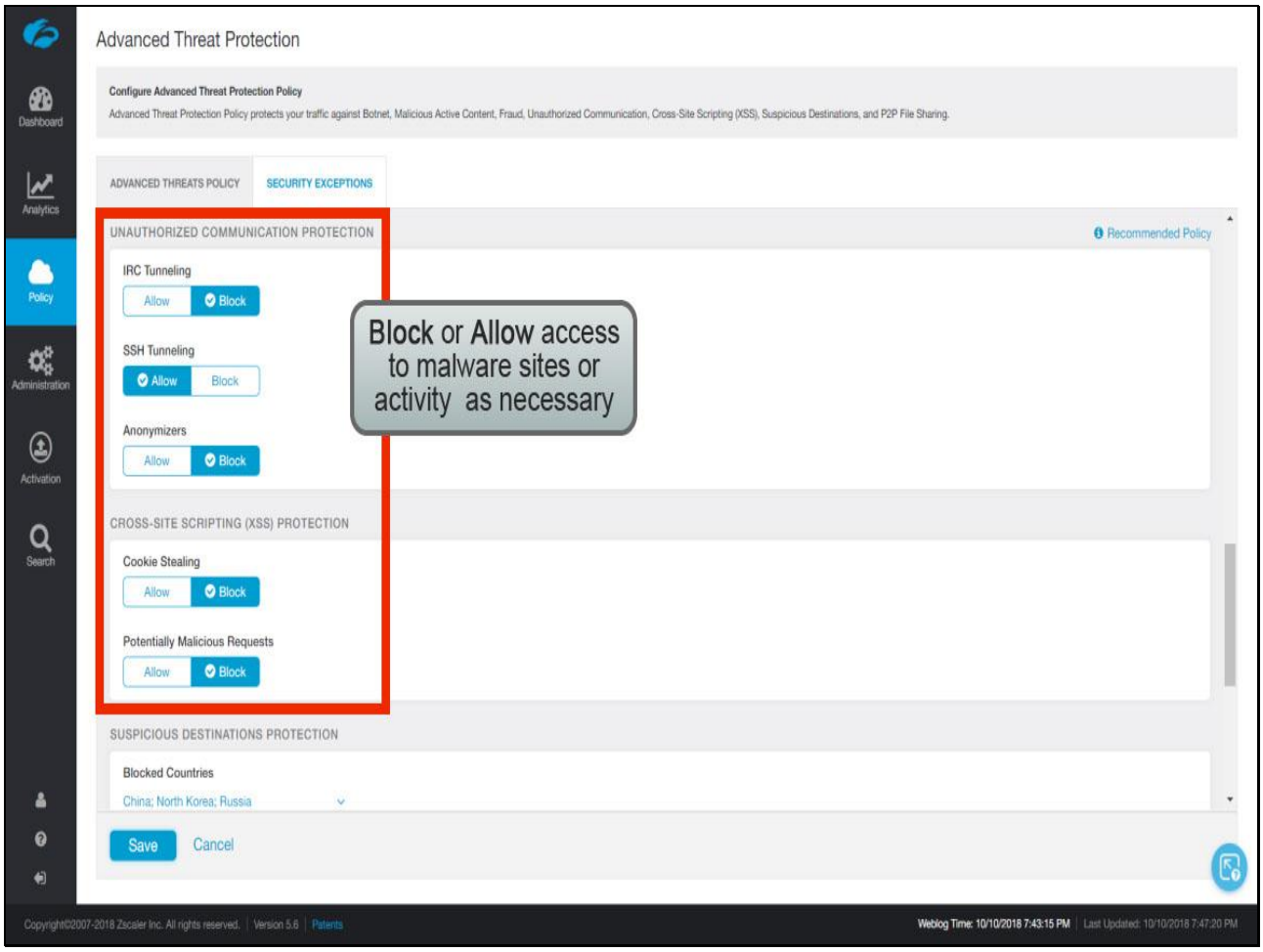
Slide 27 - Slide 27



Slide notes

The next sections are ‘FRAUD PROTECTION’, …

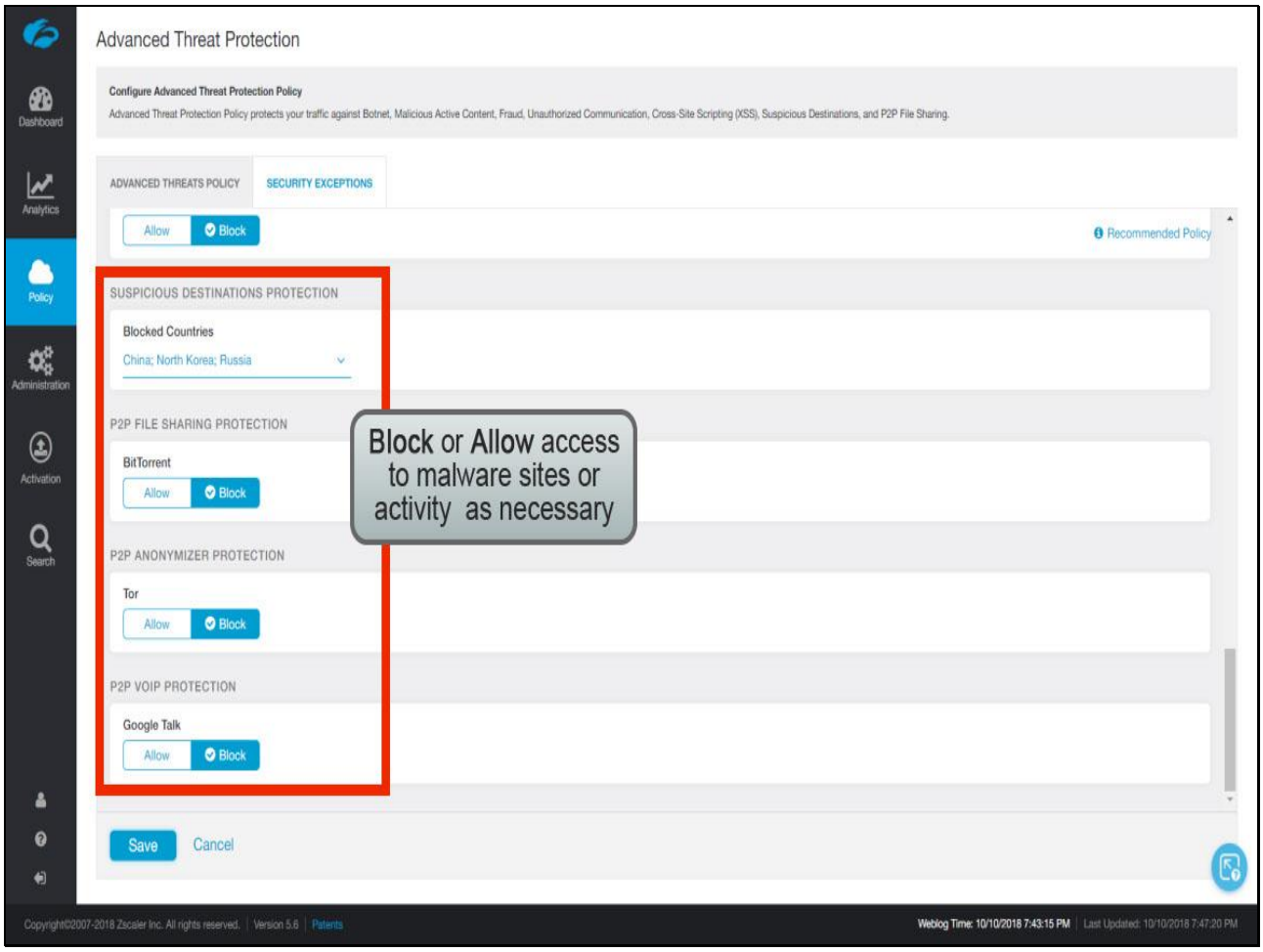
Slide 28 - Slide 28



Slide notes

…'UNAUTHORIZED COMMUNICATION PROTECTION', 'CROSS-SITE SCRIPTING (XSS) PROTECTION', …

Slide 29 - Slide 29

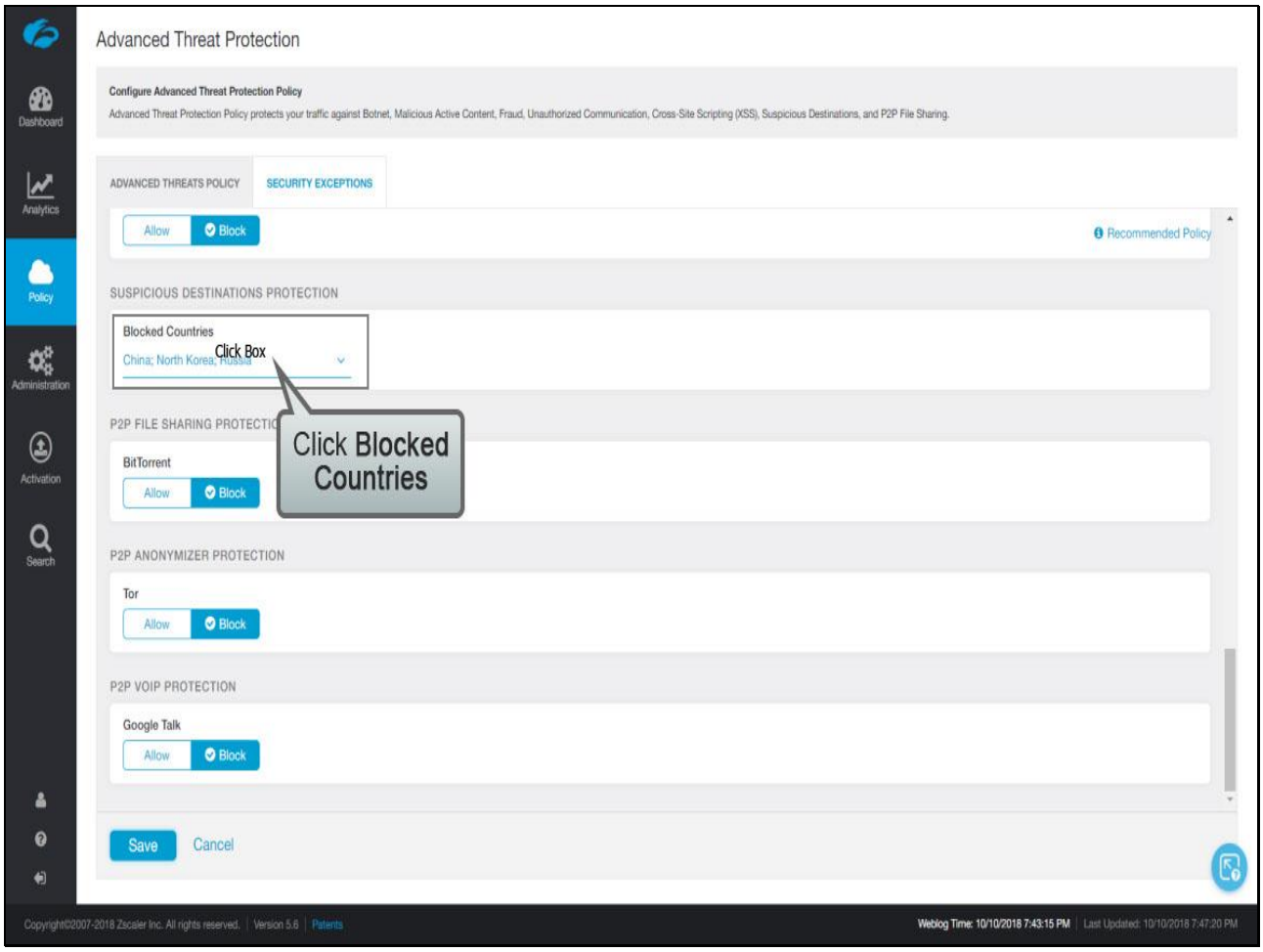


Slide notes

…'SUSPICIOUS DESTINATIONS PROTECTION', plus a set of 'P2P PROTECTION' settings (for Peer-to-Peer connections).

We recommend leaving all these at the default 'Block' option, unless you have a specific need.

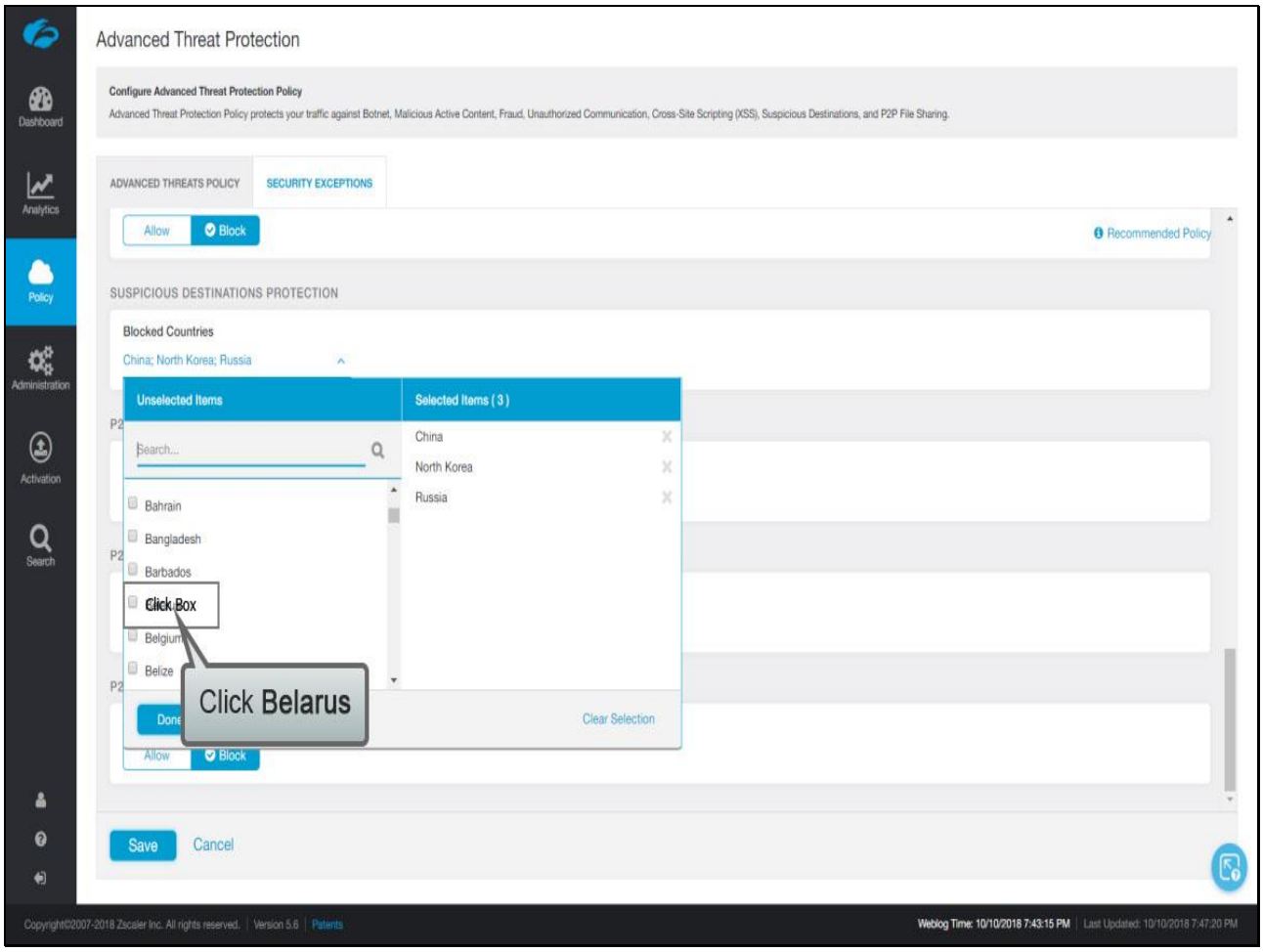
Slide 30 - Slide 30



Slide notes

In addition, you can block entire countries if necessary, based on the ISO3166 mapping of countries to their IP address space. This has the effect of blocking all traffic to, or from any IP addresses owned by the countries listed. To add a country to the block list, click in the 'Blocked Countries' field, …

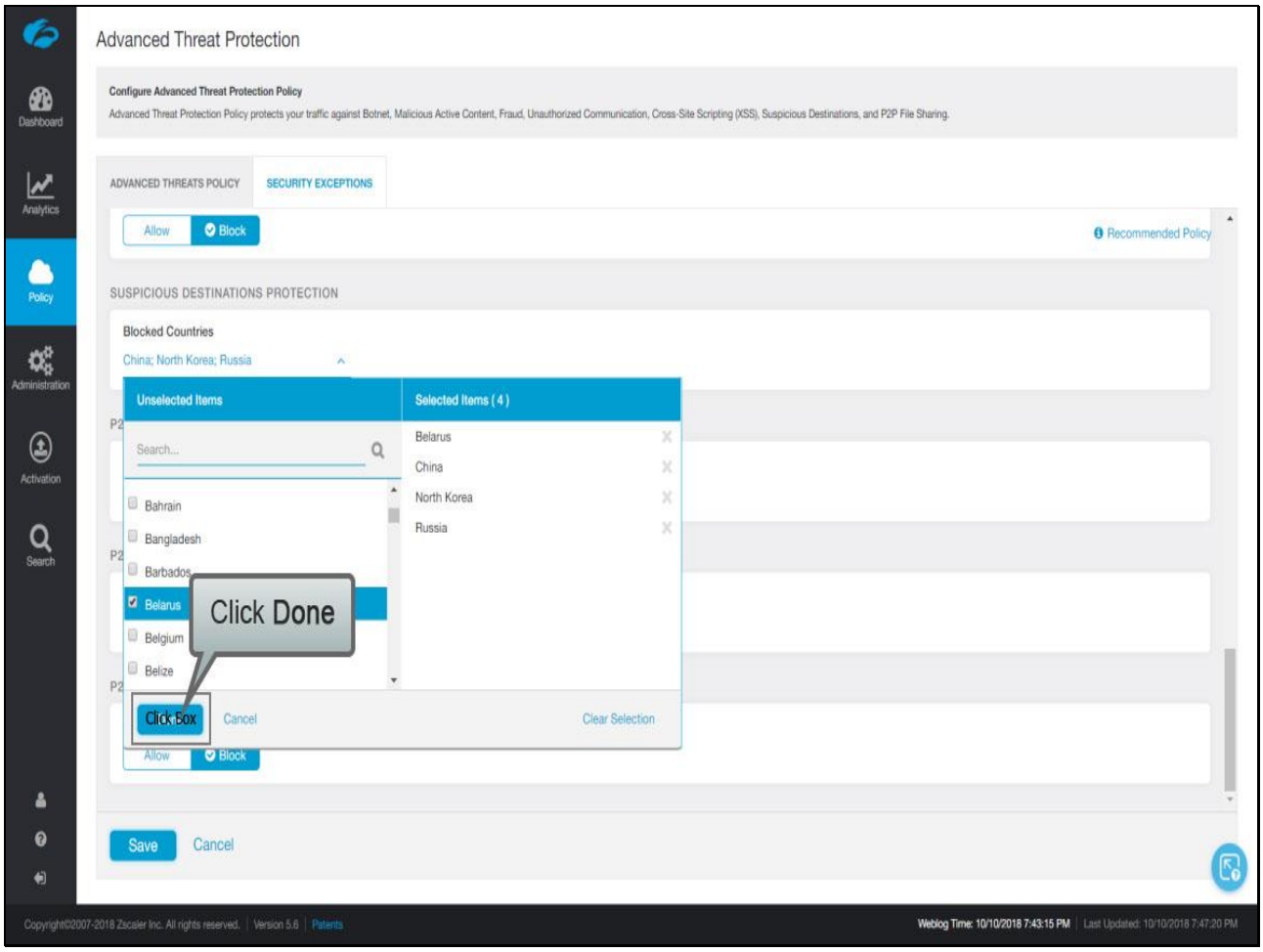
Slide 31 - Slide 31



Slide notes

…and click to select the country, or countries to add (in this case ‘Belarus’).

Slide 32 - Slide 32

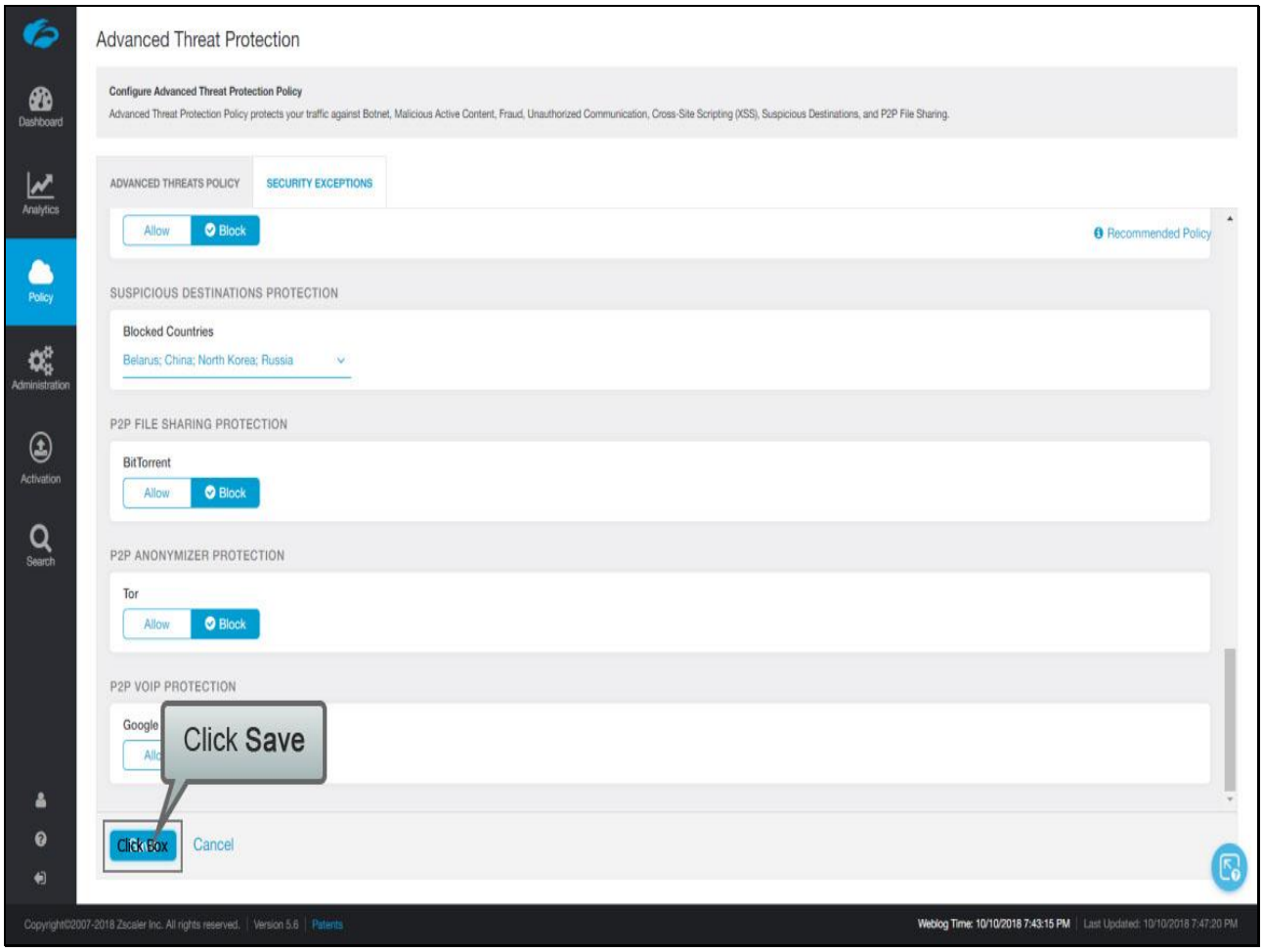


Slide notes

Note that ‘Whitelisted URLs’ take precedence over this list. If a white listed URL is hosted on a web server in a blocked country, the service will still allow users to download content from that site.

Having made changes to this policy, click ‘Done’, …

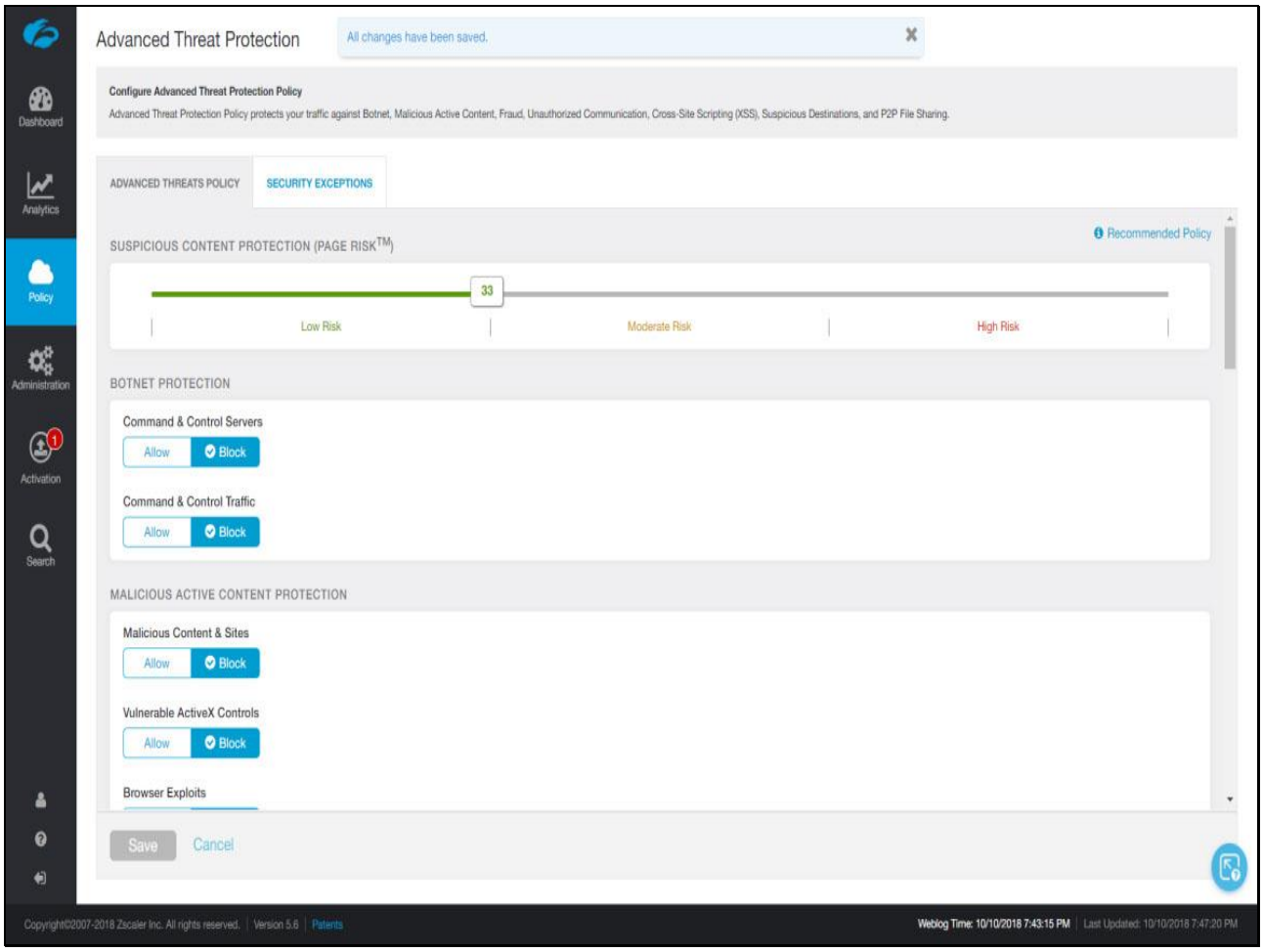
Slide 33 - Slide 33



Slide notes

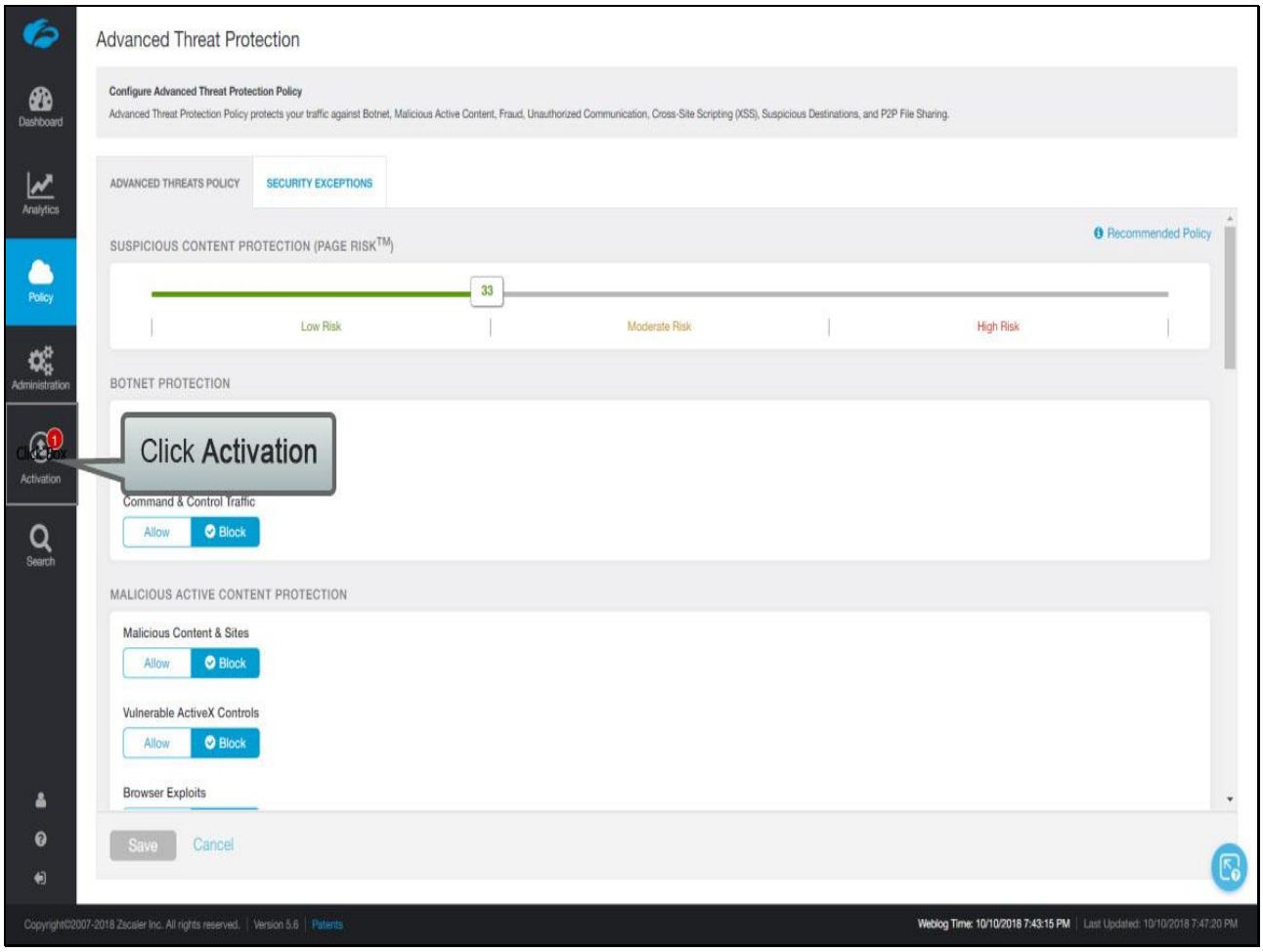
…then click ‘Save’.

Slide 34 - Slide 34



Slide notes

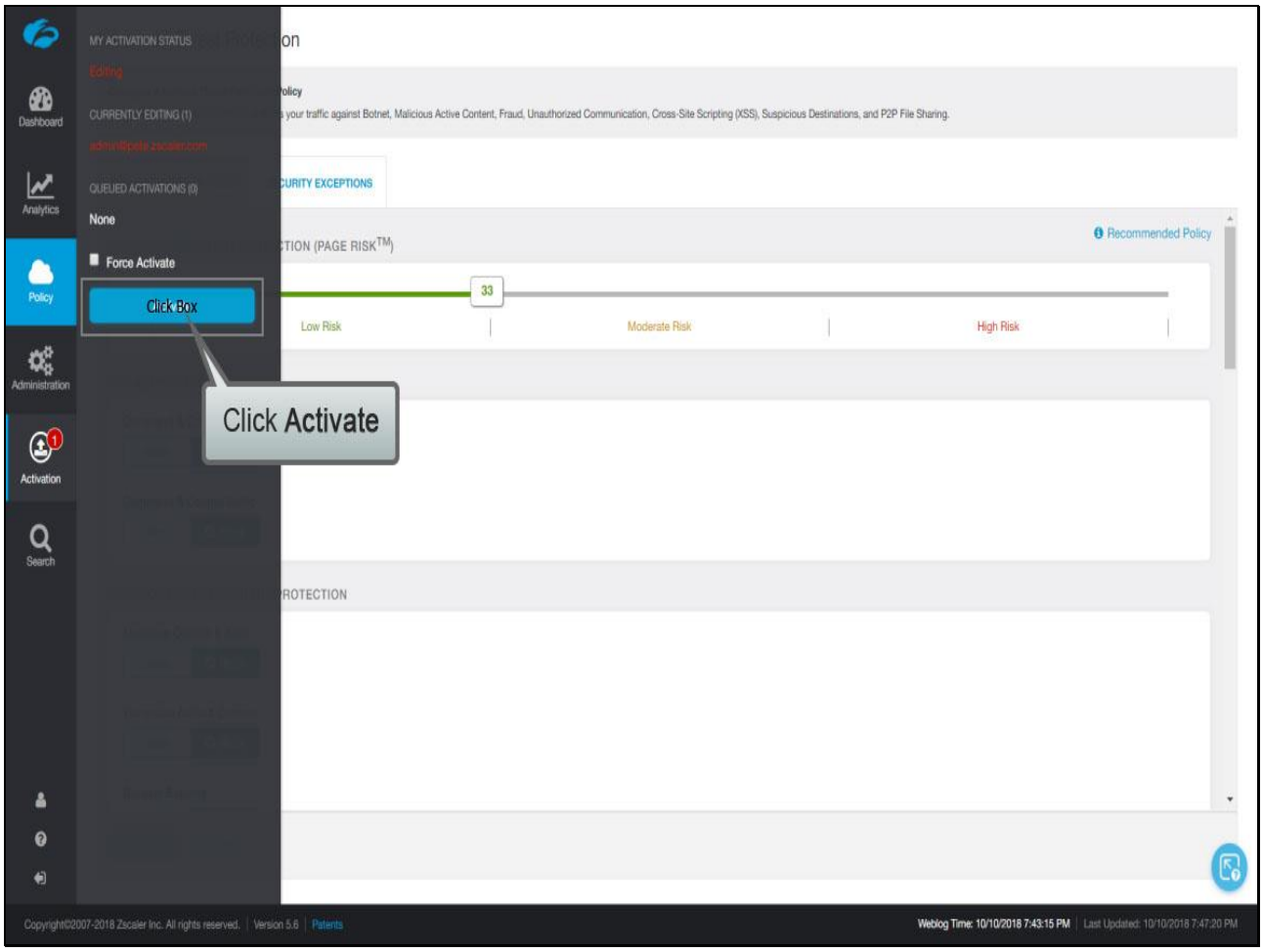
Slide 35 - Slide 35



Slide notes

Then to activate your changes, click ‘Activation’, …

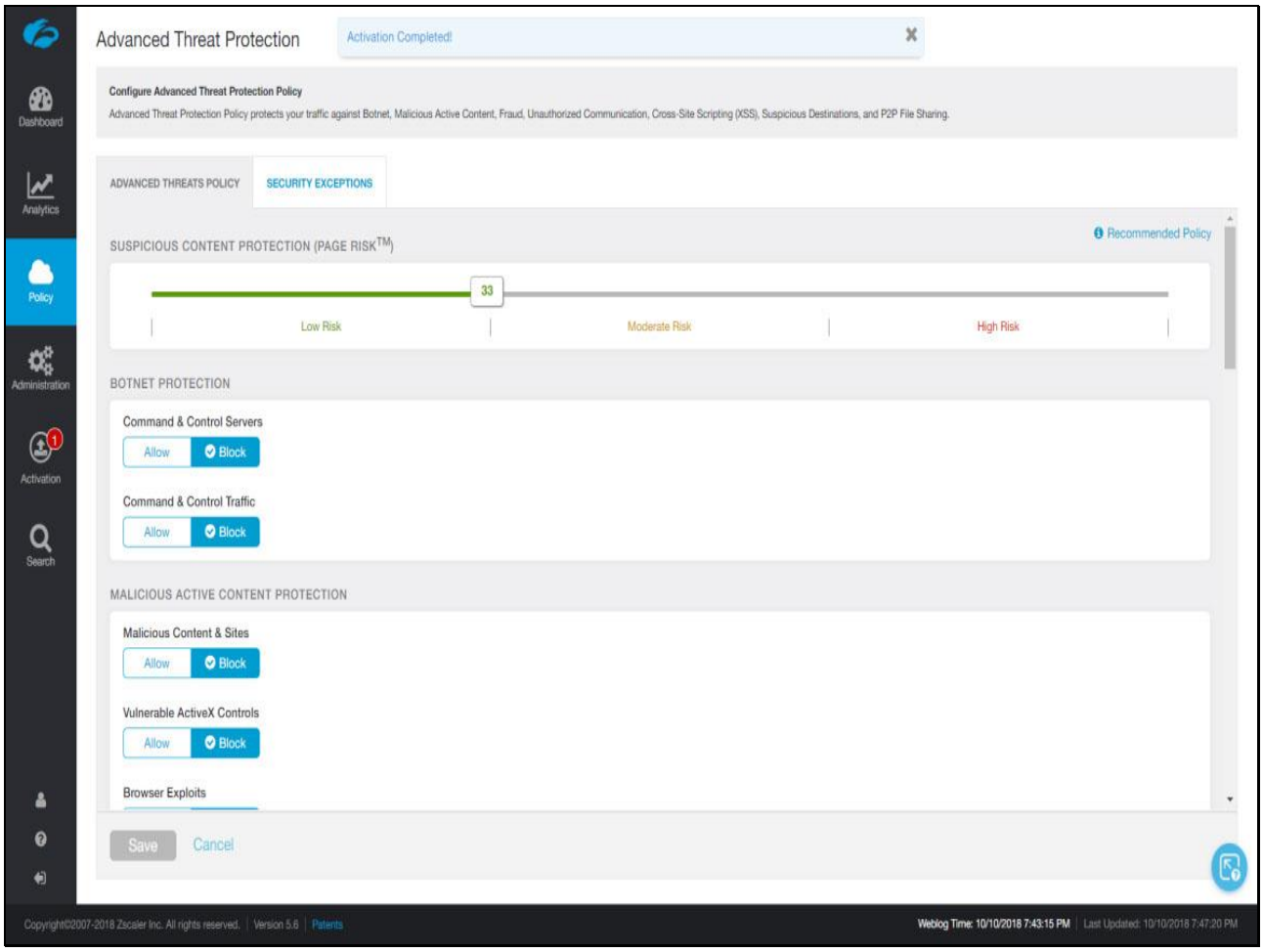
Slide 36 - Slide 36



Slide notes

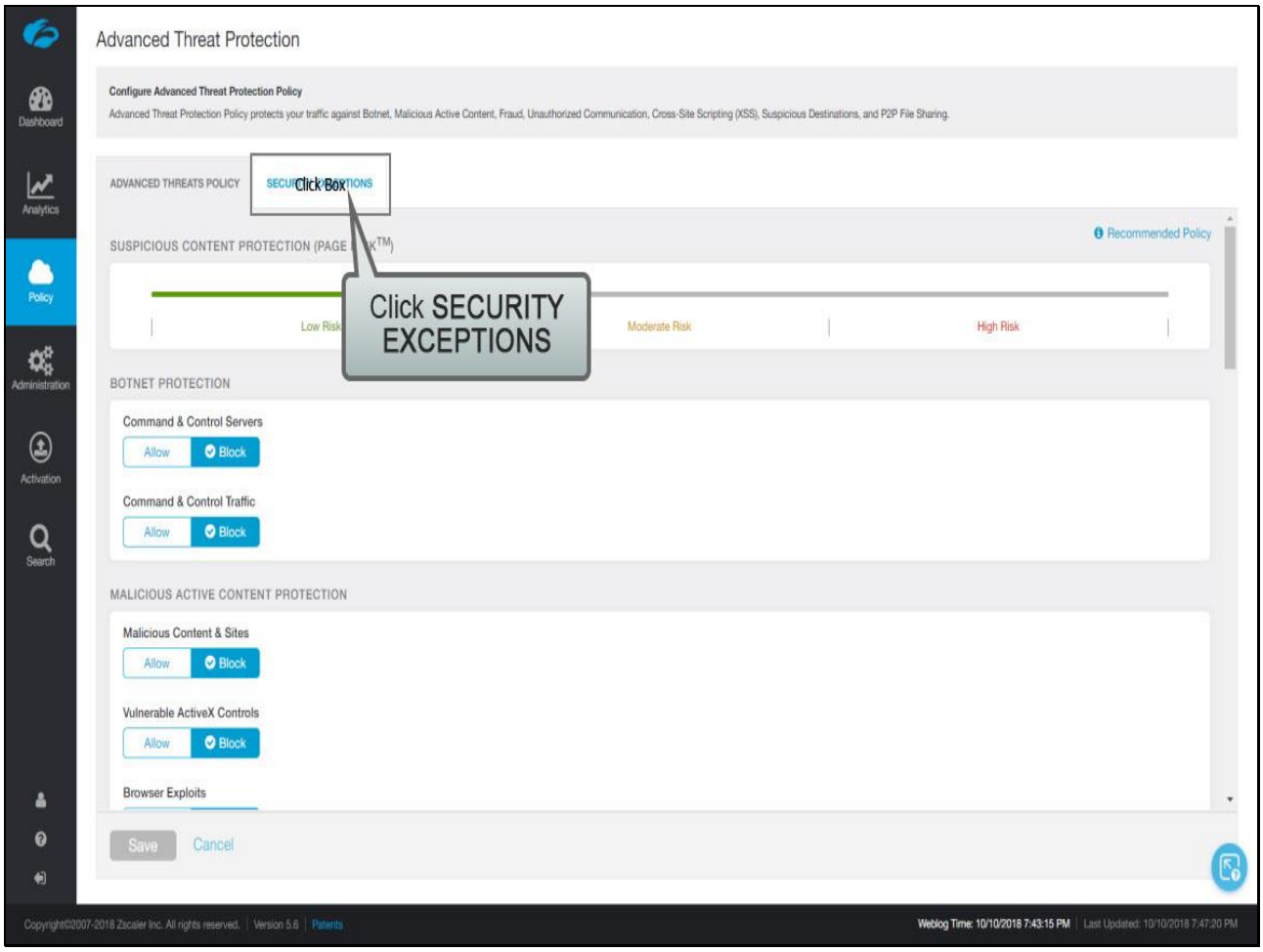
…and click ‘Activate’.

Slide 37 - Slide 37



Slide notes

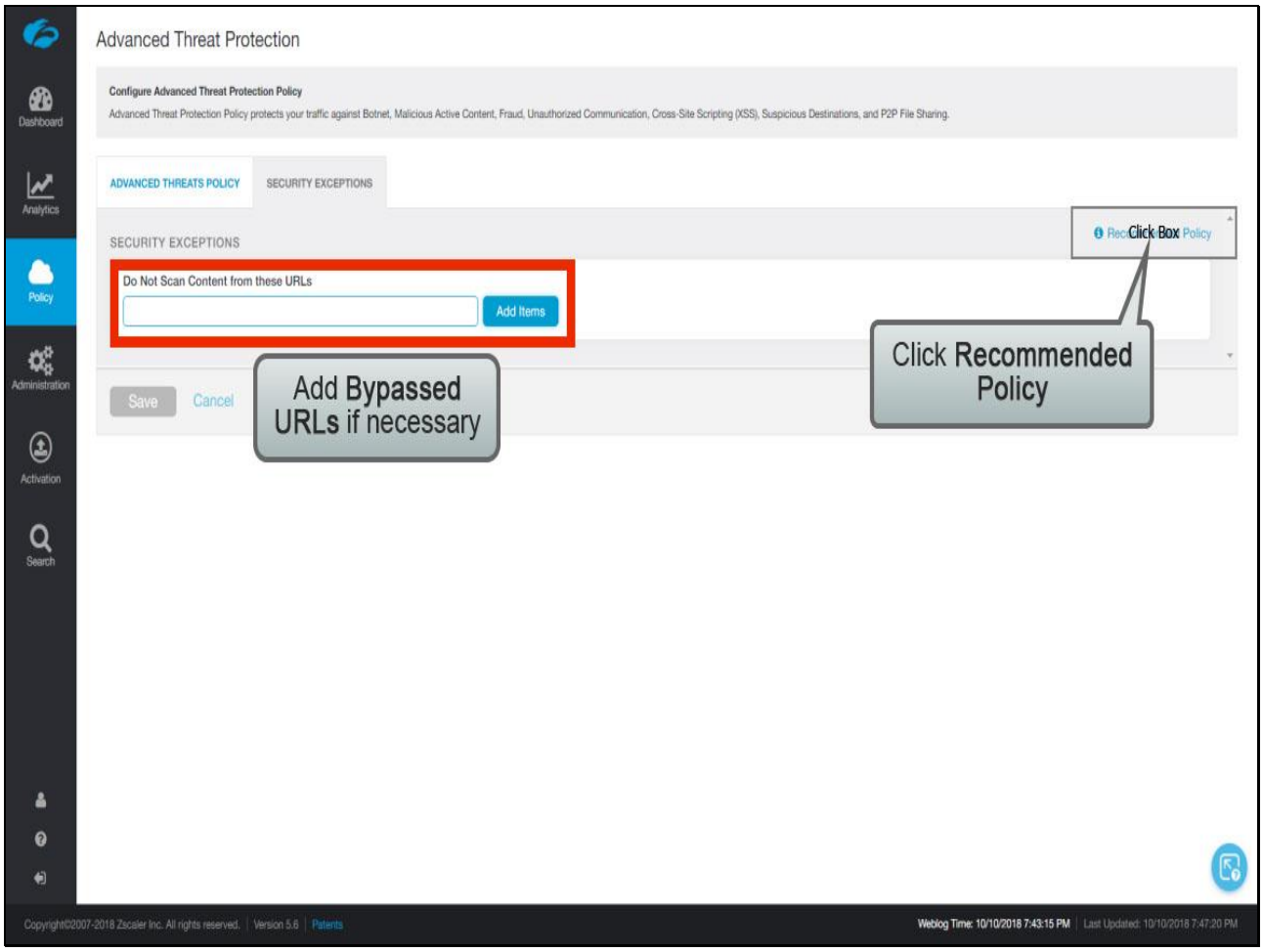
Slide 38 - Slide 38



Slide notes

You can configure exceptions to the ‘Advanced Threat Protection’ Policy, and this is done by clicking on the ‘SECURITY EXCEPTIONS’ tab.

Slide 39 - Slide 39

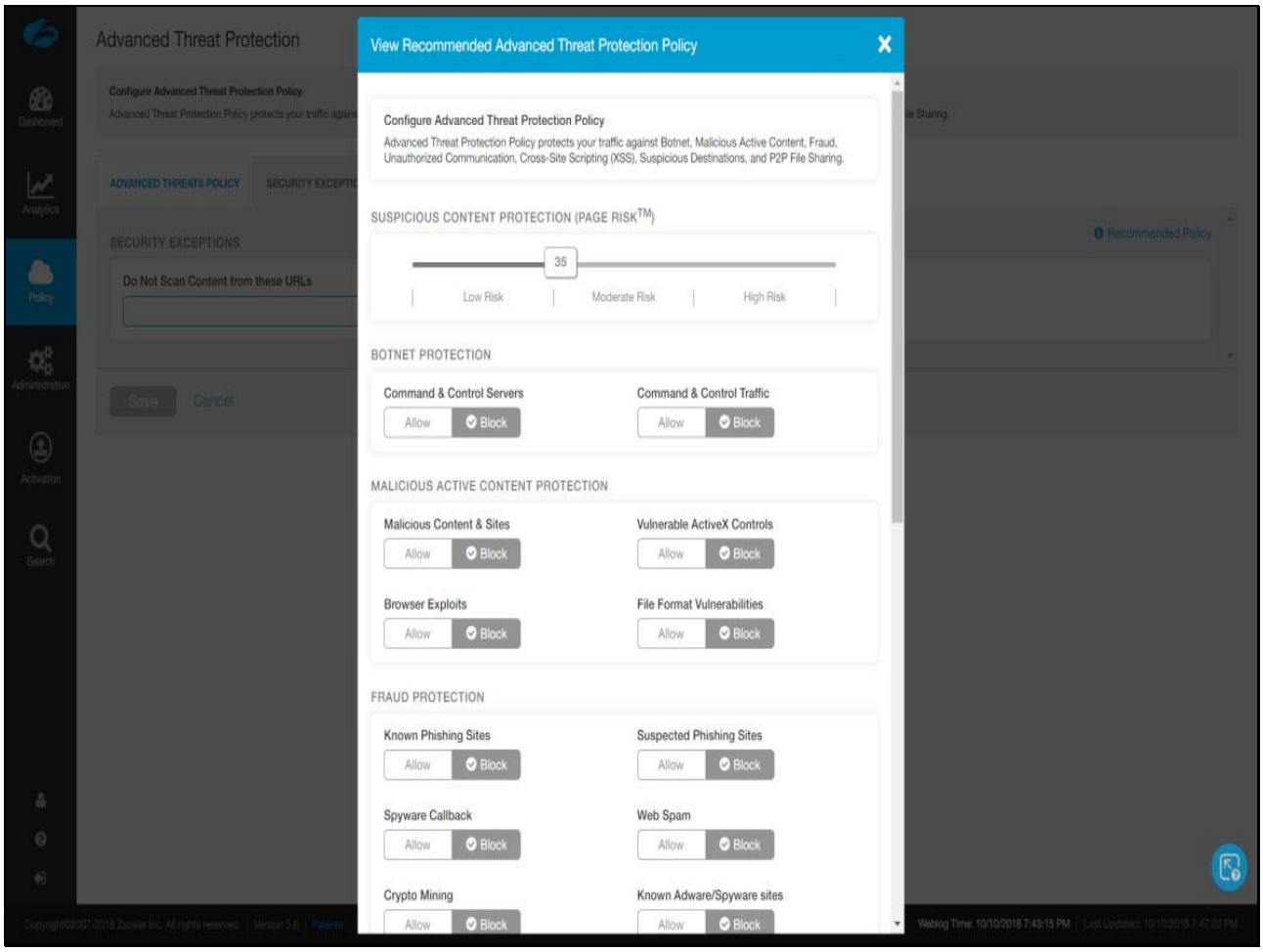


Slide notes

In this case, only a 'Do Not Scan Content from these URLs' configuration can be added as an exception. Once again, the syntax for adding URLs here is exactly the same as for the 'Do Not Scan' list that we looked at under 'Malware Protection'.

To see Zscaler recommendations for configuring 'Advanced Threat Protection' Policy settings, click the 'Recommended Policy' link.

Slide 40 - Slide 40

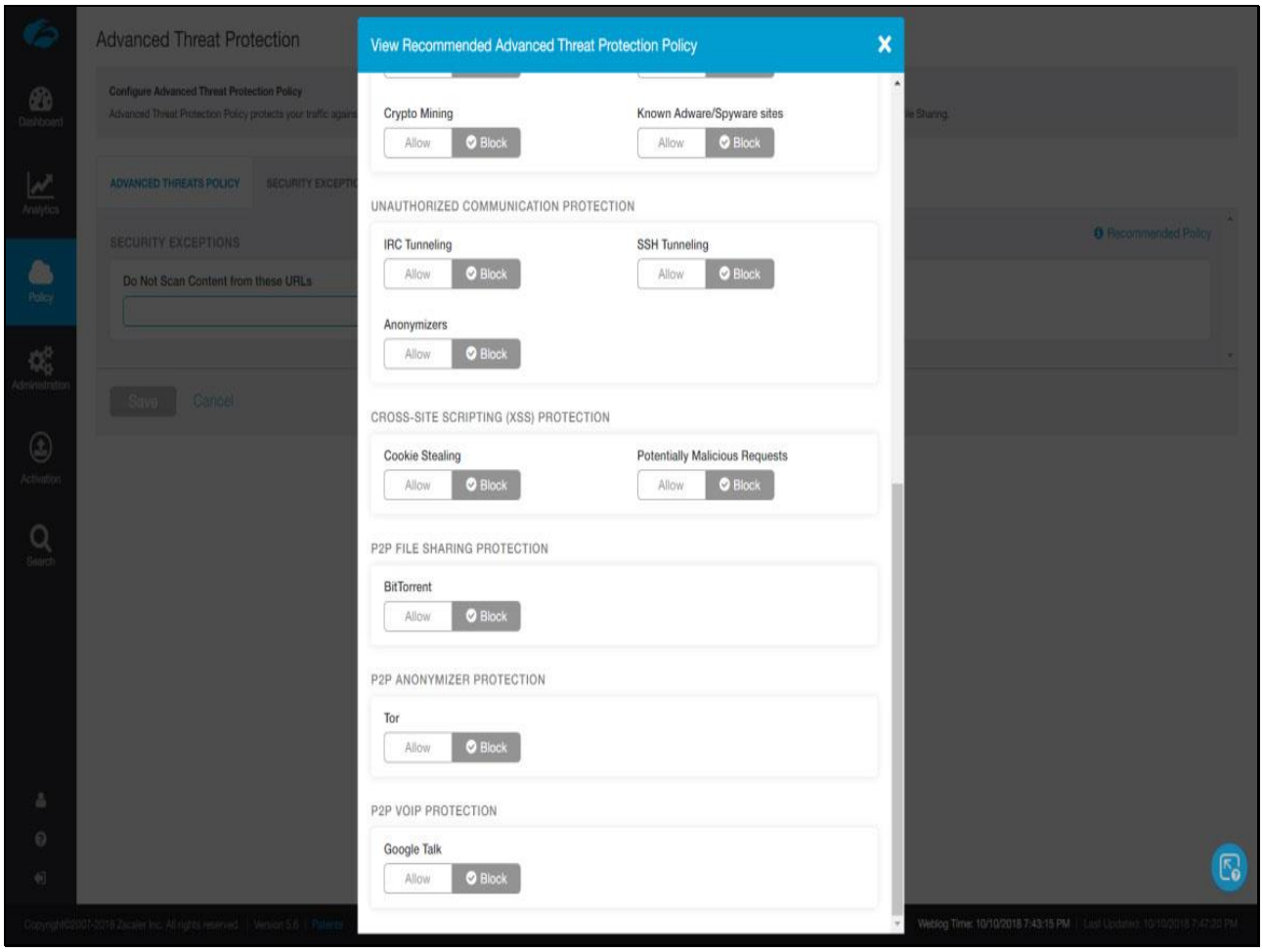


Slide notes

For the 'Advanced Threat Protection' Policy, Zscaler recommends that you:

- Set the page risk index to the 'Low Risk' area of the scale (the default level is 33);
- Block all of the advanced threats;
- And do not add any exceptions.

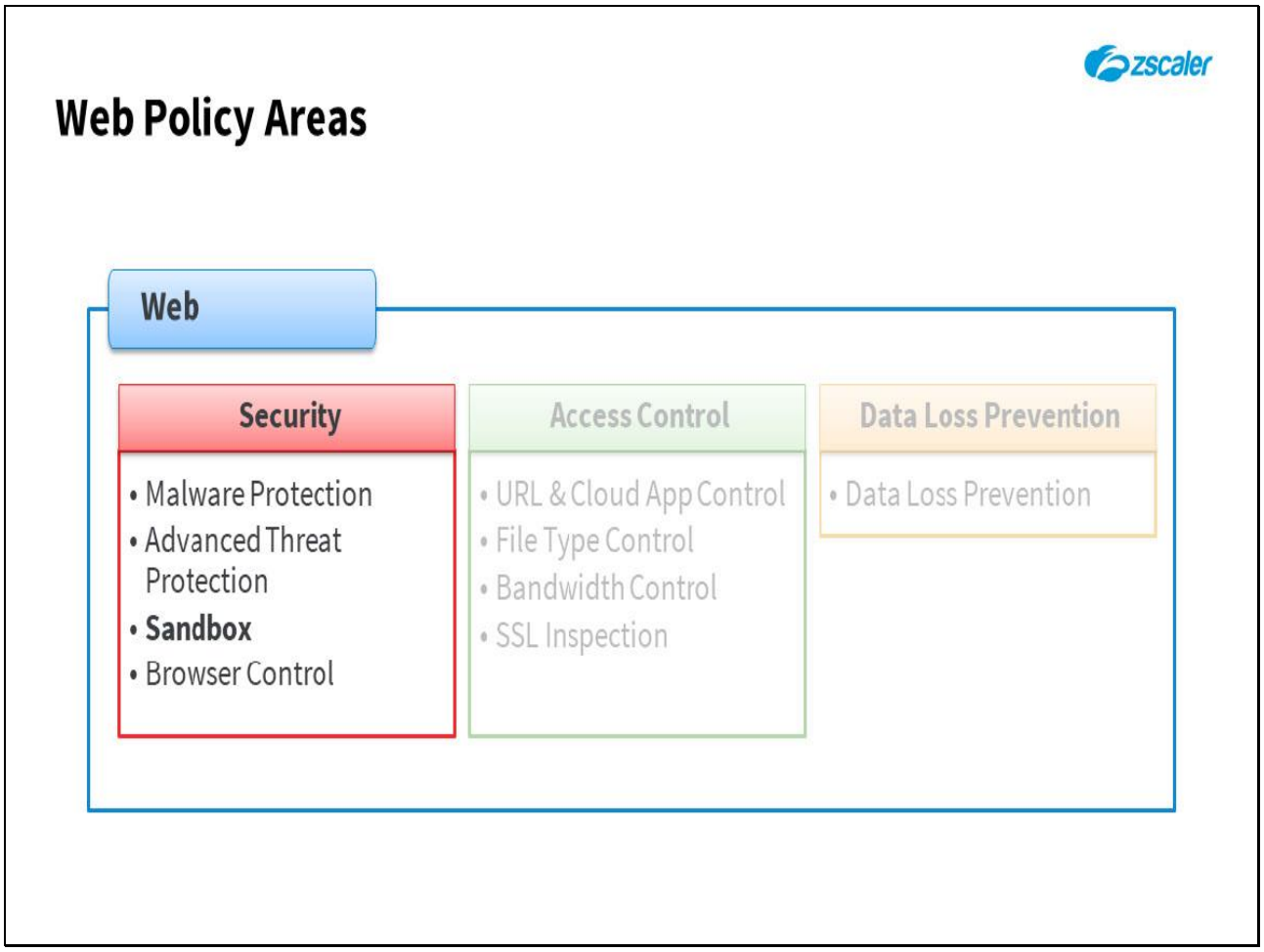
Slide 41 - Slide 41



Slide notes

One thing to note though, some peer-to-peer applications like Google Talk, or Skype would need to be explicitly enabled in this policy.

Slide 42 - Web Policy Areas



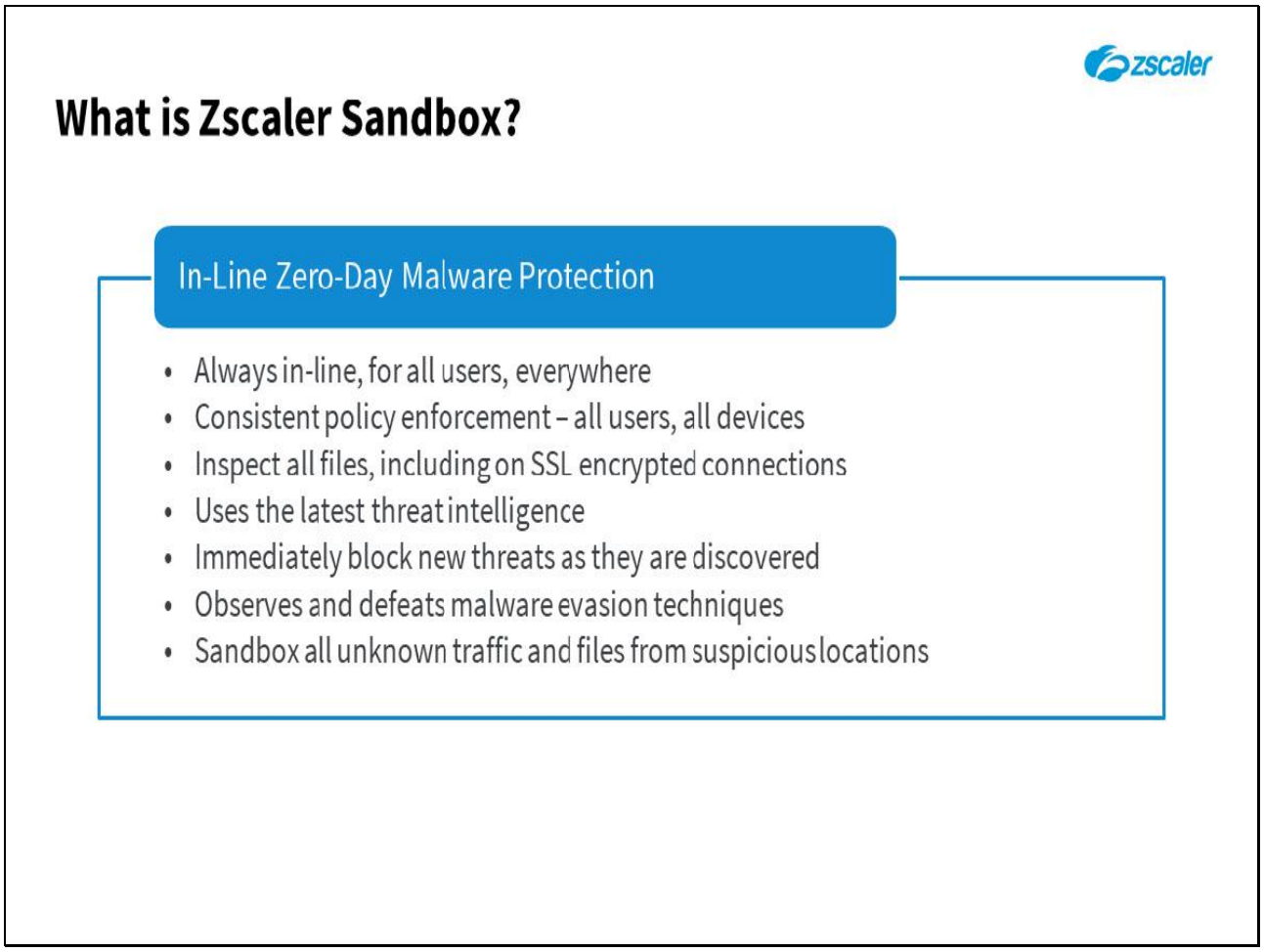
Slide notes

The 'Sandbox' Policy allows the creation of rules for the scanning and execution of files in a Zscaler sandbox environment, to be sure that any malicious content is 'detonated' safely. This provides an additional layer of security against 0-day, and Advanced Persistent Threats (APTs).

Sandbox policy rules are evaluated in the order listed, and rule evaluation stops at the first match. There is a default 'Allow and Scan' rule for all the Sandbox categories.

A detailed report on any files found to be malicious is available through the logs, a 'SANDBOX PATIENT 0 EVENTS' widget is available on the 'Security' Dashboard, plus email alerts on any discovered 0 Day threats can be configured.

Slide 43 - What is Zscaler Sandbox?

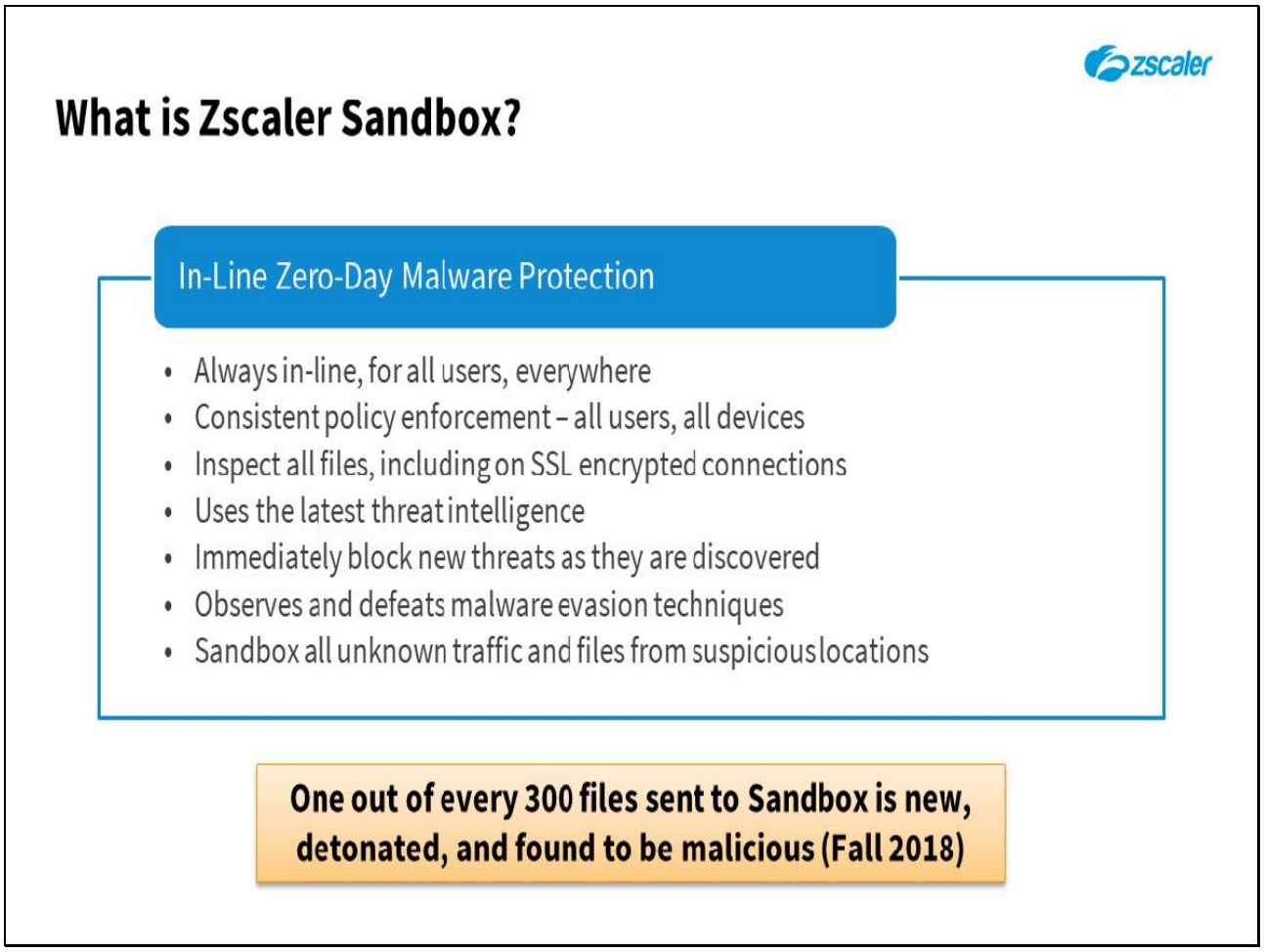


Slide notes

The Zscaler Cloud Sandbox service allows you to detect and neutralize even 'Zero-Day' threats. Because Zscaler's Sandbox service is in-line, it sits between your users and the internet no matter where they connect from, to analyze unknown files for zero-day and advanced threats. Cover every user regardless of location from the cloud, whether on or off network everyone gets the exact same protection, without cumbersome VPNs or costly MPLS links. We can even inspect incoming files on SSL encrypted connections to ensure we detect and neutralize all inbound zero-day threats.

As with all our services we make use the latest threat intelligence, plus we can detect previously unreported threats by 'detonating' an unknown file in our sandbox environment, to see what it does and what traffic it may generate (e.g. botnet communications or attempted data extraction). We even recognize and neutralize attempts by malware to evade sandbox detection. All unknown files from suspicious locations will be sandboxed, including the blocking of all executable files.

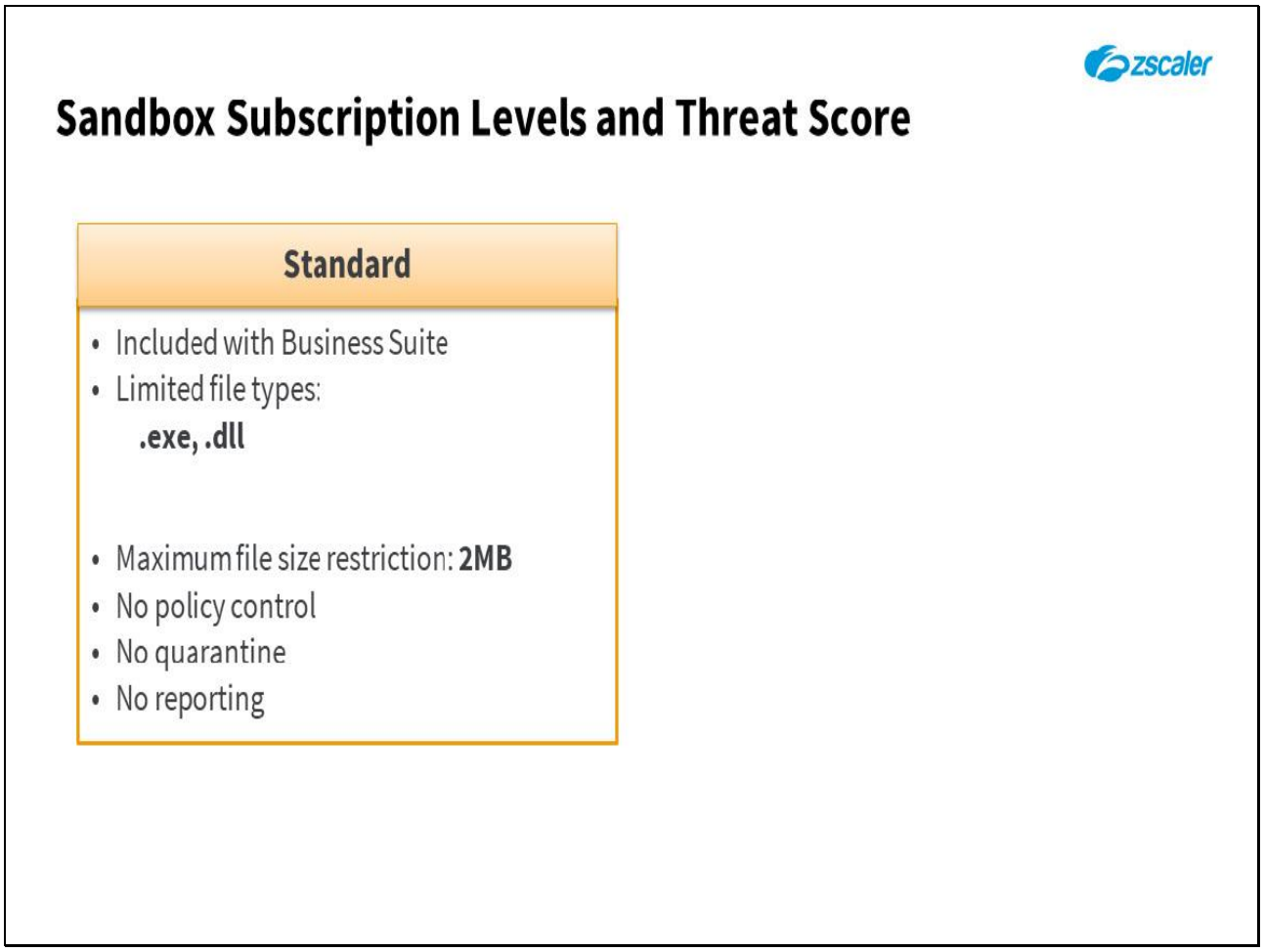
Slide 44 - What is Zscaler Sandbox?



Slide notes

Note that currently (Fall 2018), we find that 1 in every 300 files sent to our Cloud Sandbox, are found to be malicious when detonated.

Slide 45 - Sandbox Subscription Levels and Threat Score

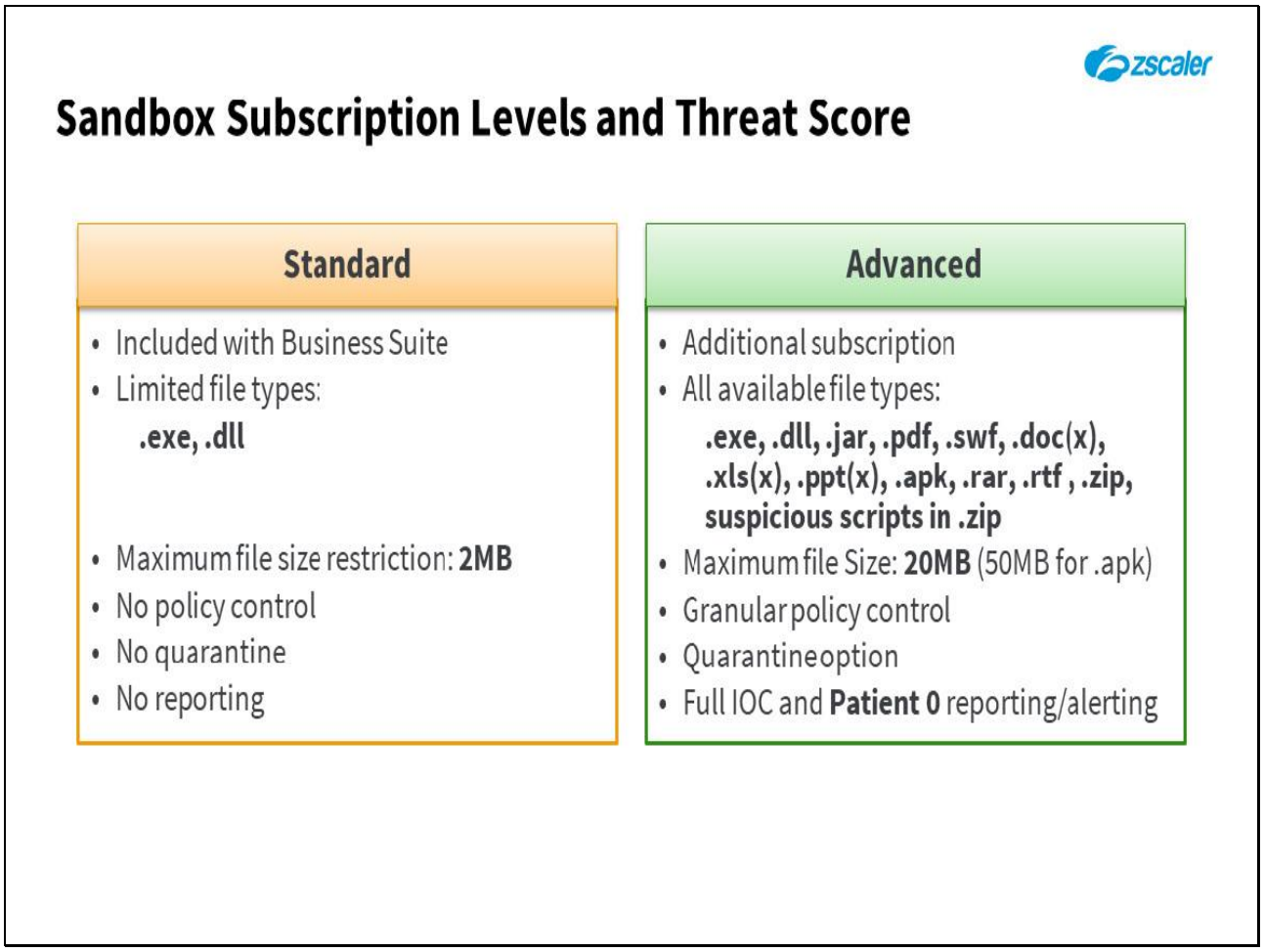


Slide notes

The 'Standard' Sandbox subscription is included with our 'Business Suite' and provides a basic level of protection against zero-day threats:

- Only the .exe and .dll file types from 'suspicious' URL categories are scanned and blocked, the suspicious categories being: 'Misc./unknown', 'Nudity', 'Pornography', 'Web host', 'File host', 'Shareware download', and 'Anonymizer'.
- The maximum size of file that can be scanned is 2MB;
- Policy control rules cannot be created;
- There is no option to apply the 'Quarantine' action (scan and detonate the file before it is downloaded);
- And there is no detailed Sandbox reporting.

Slide 46 - Sandbox Subscription Levels and Threat Score

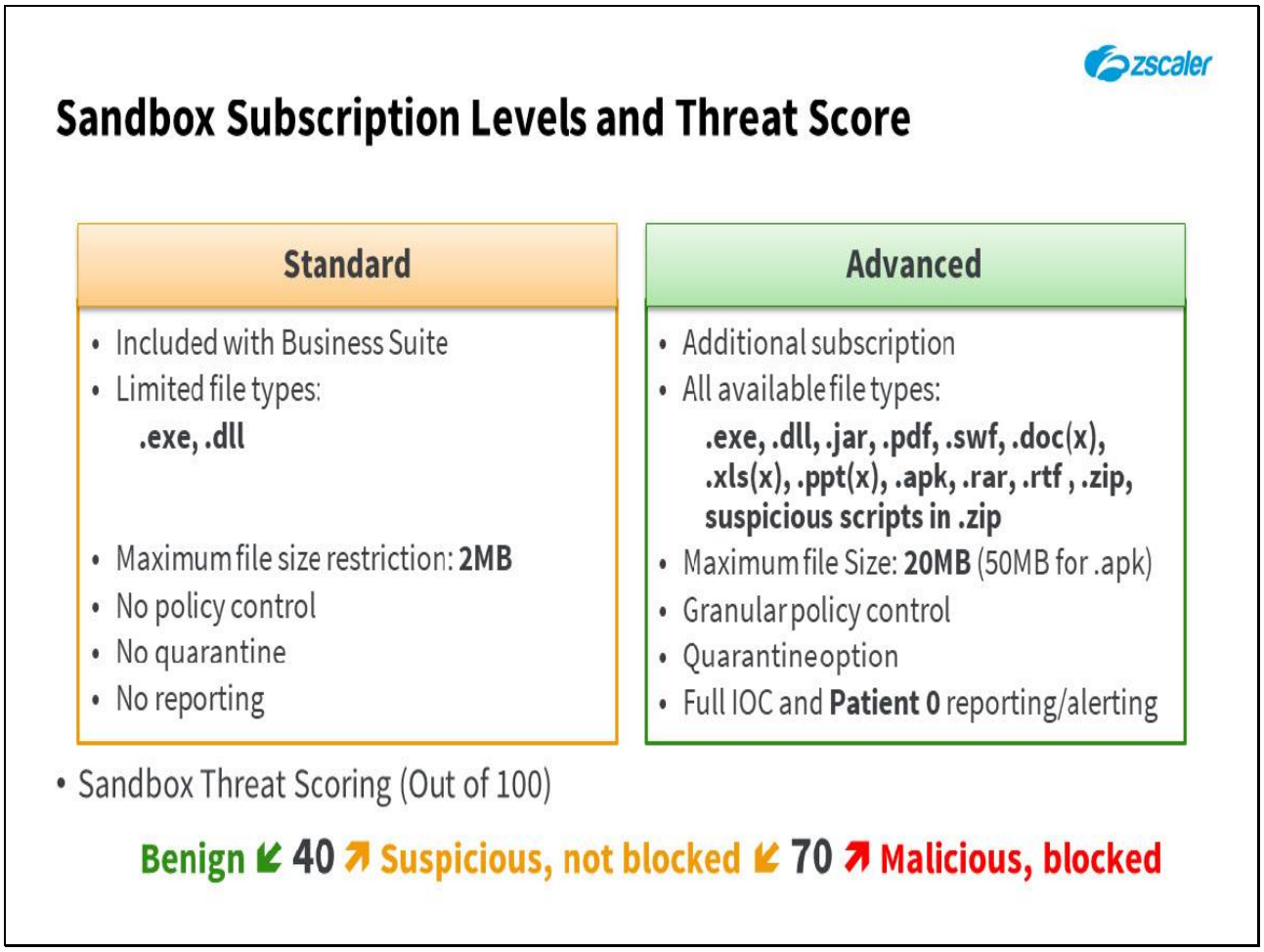


Slide notes

The 'Advanced' Sandbox subscription provides a much more comprehensive level of zero-day protection:

- The file types that can be scanned are: .exe, .dll, .jar, .pdf, .swf, .doc(x), .xls(x), .ppt(x), .apk, .rar, .rtf, .zip, plus any suspicious scripts within a .zip file.
- The maximum file size that can be scanned is 20MB (or 50MB for Android .apk files);
- Granular Sandbox policy rules can be created and assigned, and the 'Quarantine' action is available within them.
- Plus, there is full 'Indicator of Compromise' (IOC) reporting, as well as a 'Patient 0' widget on the 'Security' Dashboard for full visibility into newly discovered threats. Email alerts for any newly discovered 0 Day threats can be enabled and configured from the 'Administration > Alerts' page.

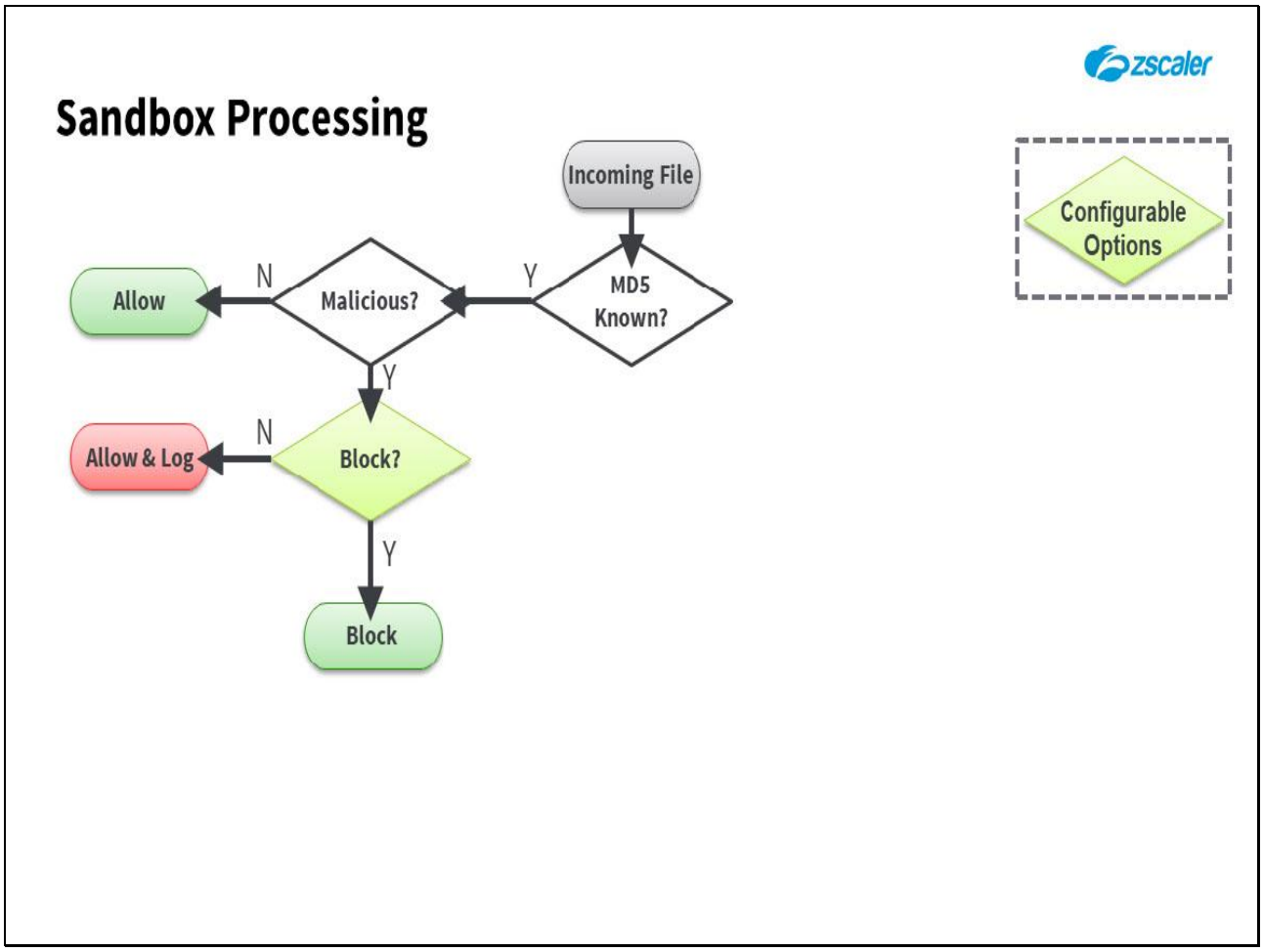
Slide 47 - Sandbox Subscription Levels and Threat Score



Slide notes

Under the covers, the Sandbox makes decisions about files based on a hard-coded 'Risk Score' (in addition to the configurable 'Page Risk Score' in the 'Advanced Threat Protection' policy). A file's 'Risk Score' is out of '100' and it is determined when analyzing the file. Anything that scores above '70' is deemed 'Malicious' and will be blocked and black-listed; anything that scores below '40' is considered 'Benign' and will be white-listed; anything in between is considered 'Suspicious' but will not be automatically blocked.

Slide 48 - Sandbox Processing



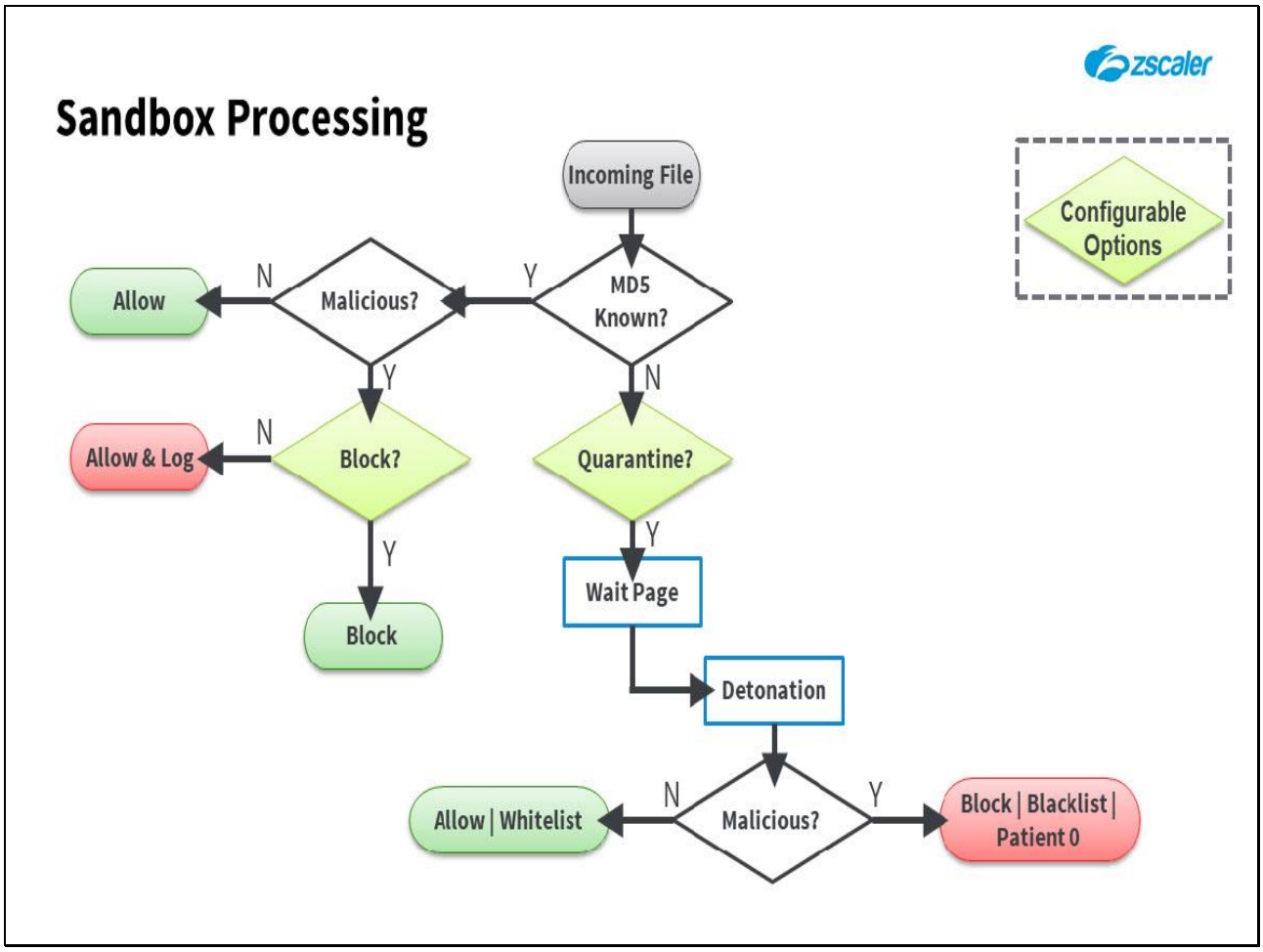
Slide notes

The processing flow for our Cloud Sandbox starts when we detect an incoming file, and if the MD5 hash for the file is already known, we can make an immediate forwarding decision:

- If it is already known to be benign, we will simply allow the download;
- If it is known to be malicious you can configure the behavior, whether to simply block (the safest option), or to allow it to proceed and log the event.

If you allow and log malicious files then the service can be considered to be an 'Intrusion Detection System' only (IDS), rather than a full 'Intrusion Prevention System' (IPS).

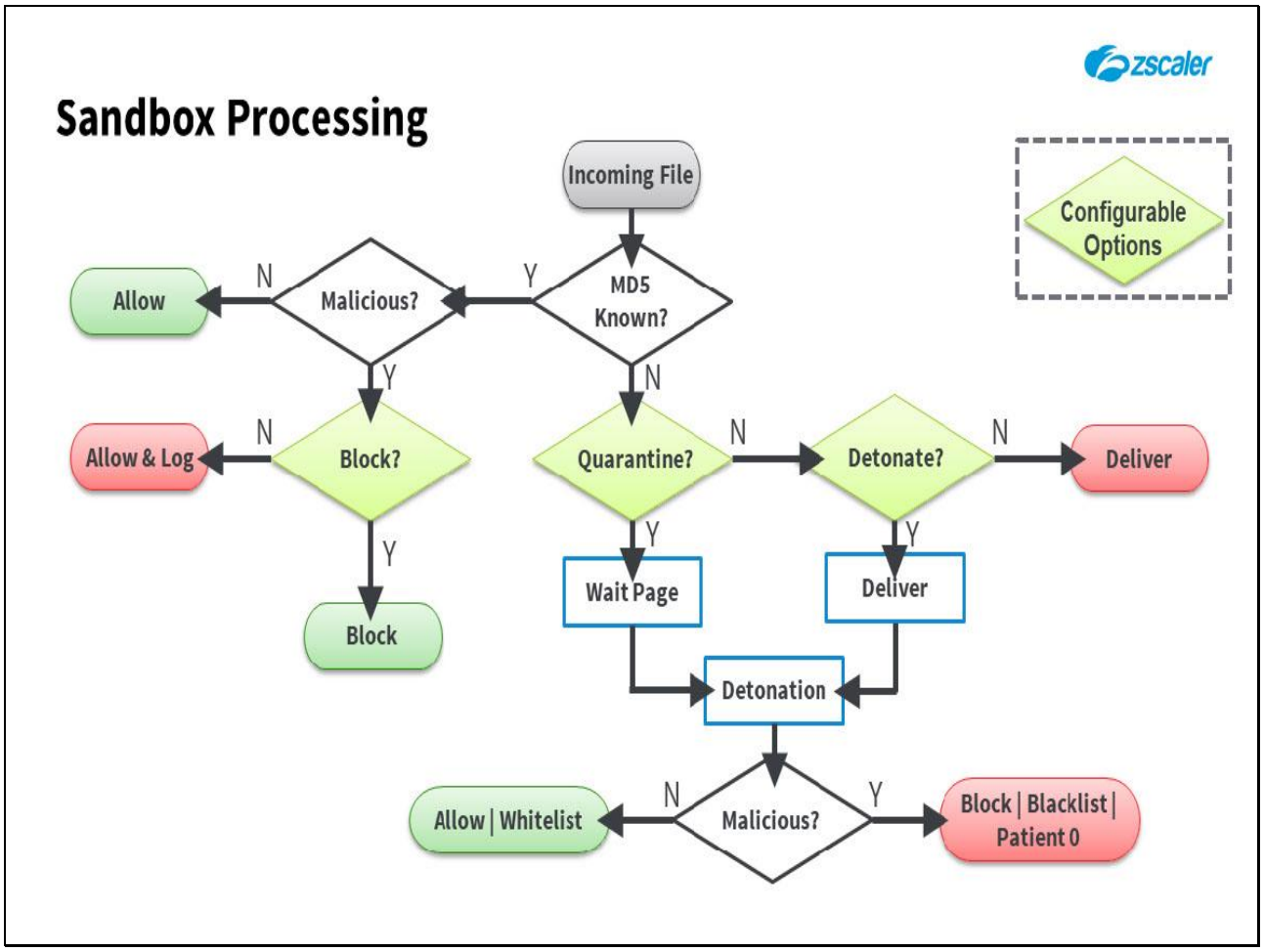
Slide 49 - Sandbox Processing



Slide notes

If the MD5 hash for the file is not known, you have the option whether or not to ‘Quarantine’ the file, i.e. block the download until the file has been proven to be benign. If you enable the ‘Quarantine’ option, we will display a ‘Wait’ page to the end user while we detonate and analyze the file. This page is refreshed at intervals and if the file is found to be OK, it will be automatically delivered. If it is found to be malicious, it will be blocked and black-listed, and a report will be posted to the ‘Patient 0’ widget on the ‘Security’ Dashboard.

Slide 50 - Sandbox Processing

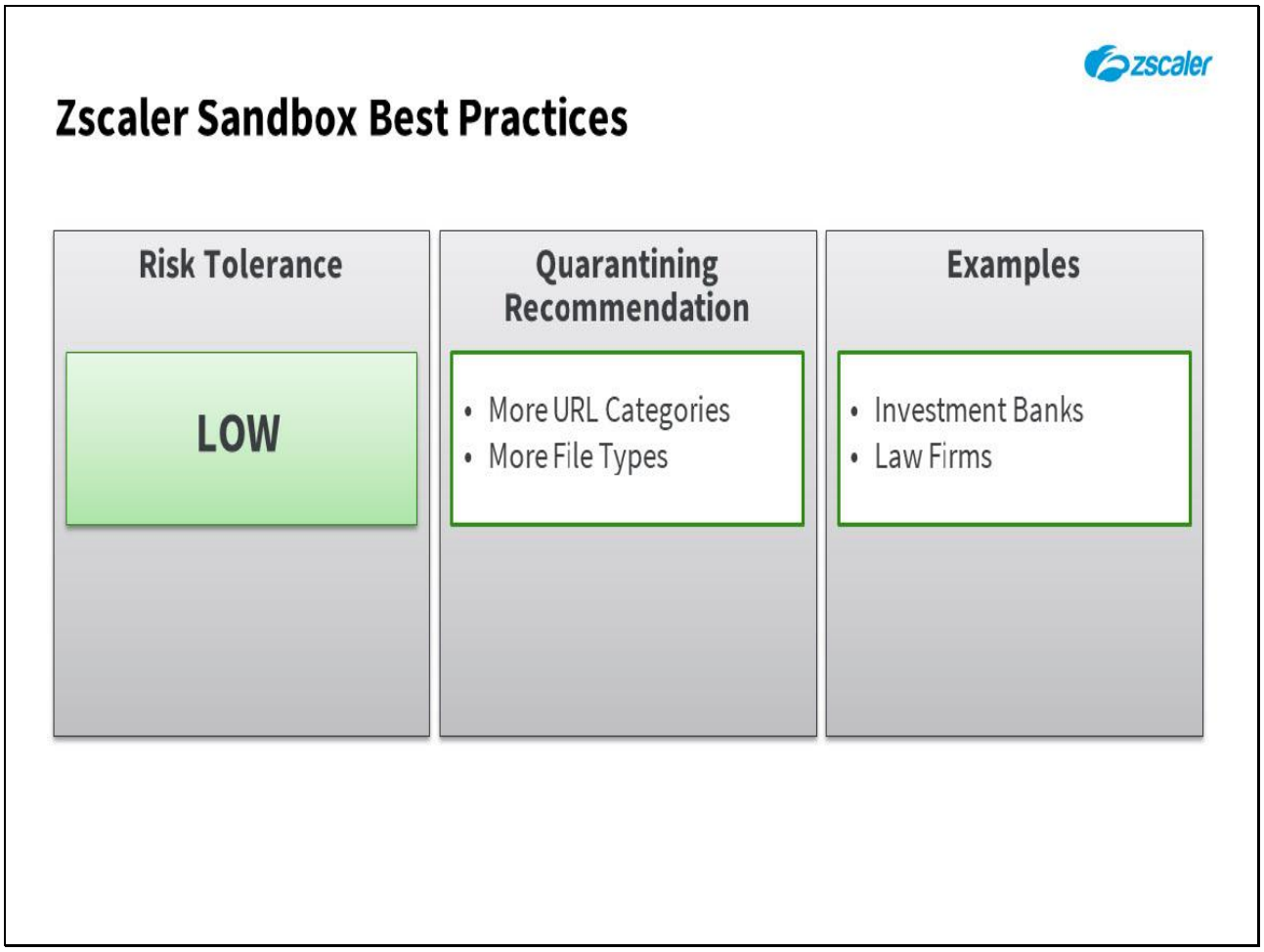


Slide notes

If you elect not to use the 'Quarantine' option, you can decide whether or not to Sandbox it at all, and if not, we simply deliver the file. Note that this would be considered a risky option, as there is no way to know whether the file is safe.

If you elect to analyze the file, we will detonate it as before although the file will be delivered to the end user regardless, while we proceed with detonation and analysis. If the file is retrospectively found to be benign, all well and good; if it is found to be malicious, it will be blocked for subsequent downloads, black-listed and a report will be posted to the 'Patient 0' widget on the 'Security' Dashboard.

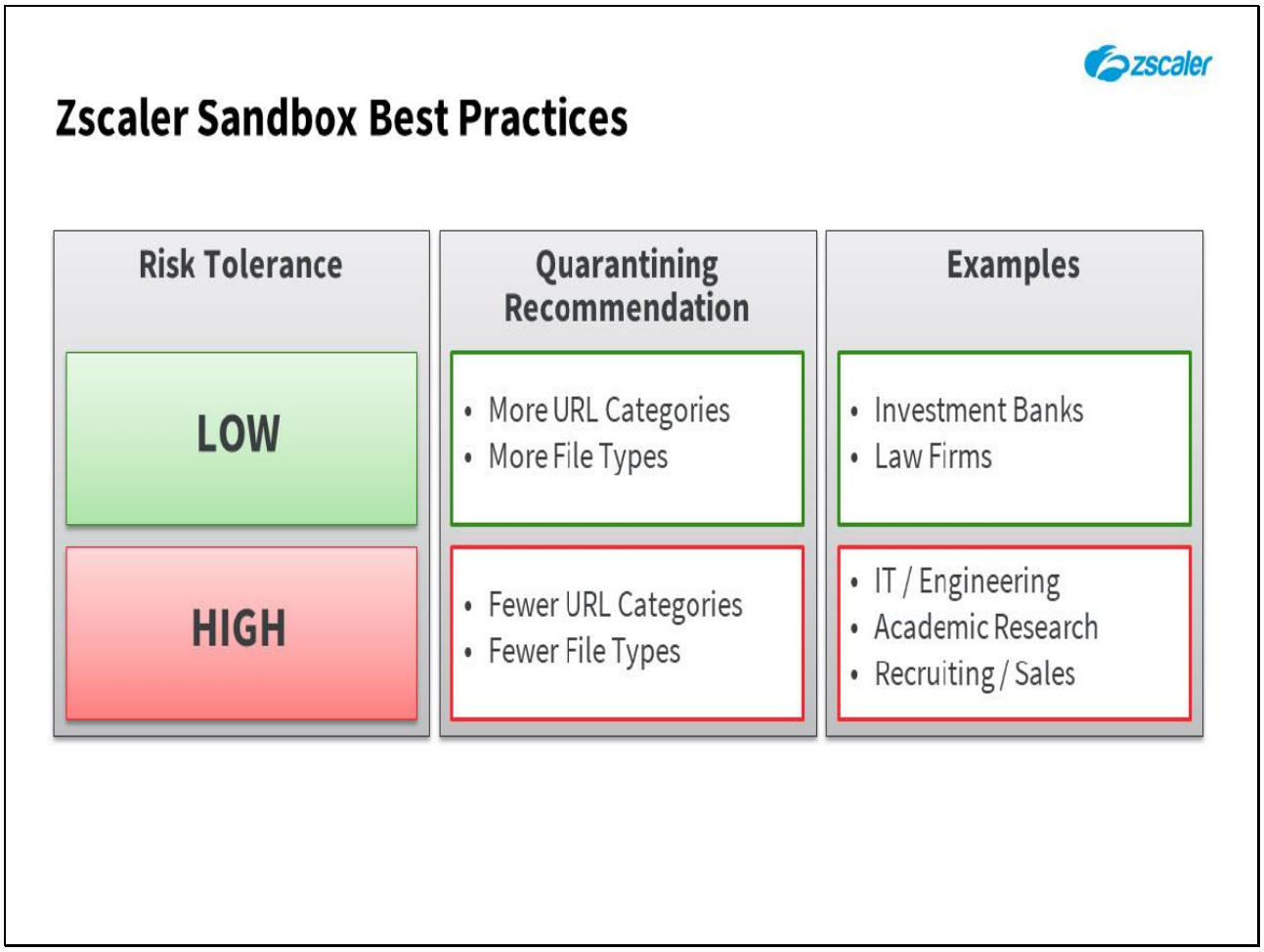
Slide 51 - Zscaler Sandbox Best Practices



Slide notes

Best practices for the Zscaler Cloud Sandbox are really determined by the tolerance to risk of the customer. Some people are very risk averse (i.e. have low risk tolerance, such as Investment Banks, or Law firms), and they would probably require many more URL Categories and file types to be analyzed.

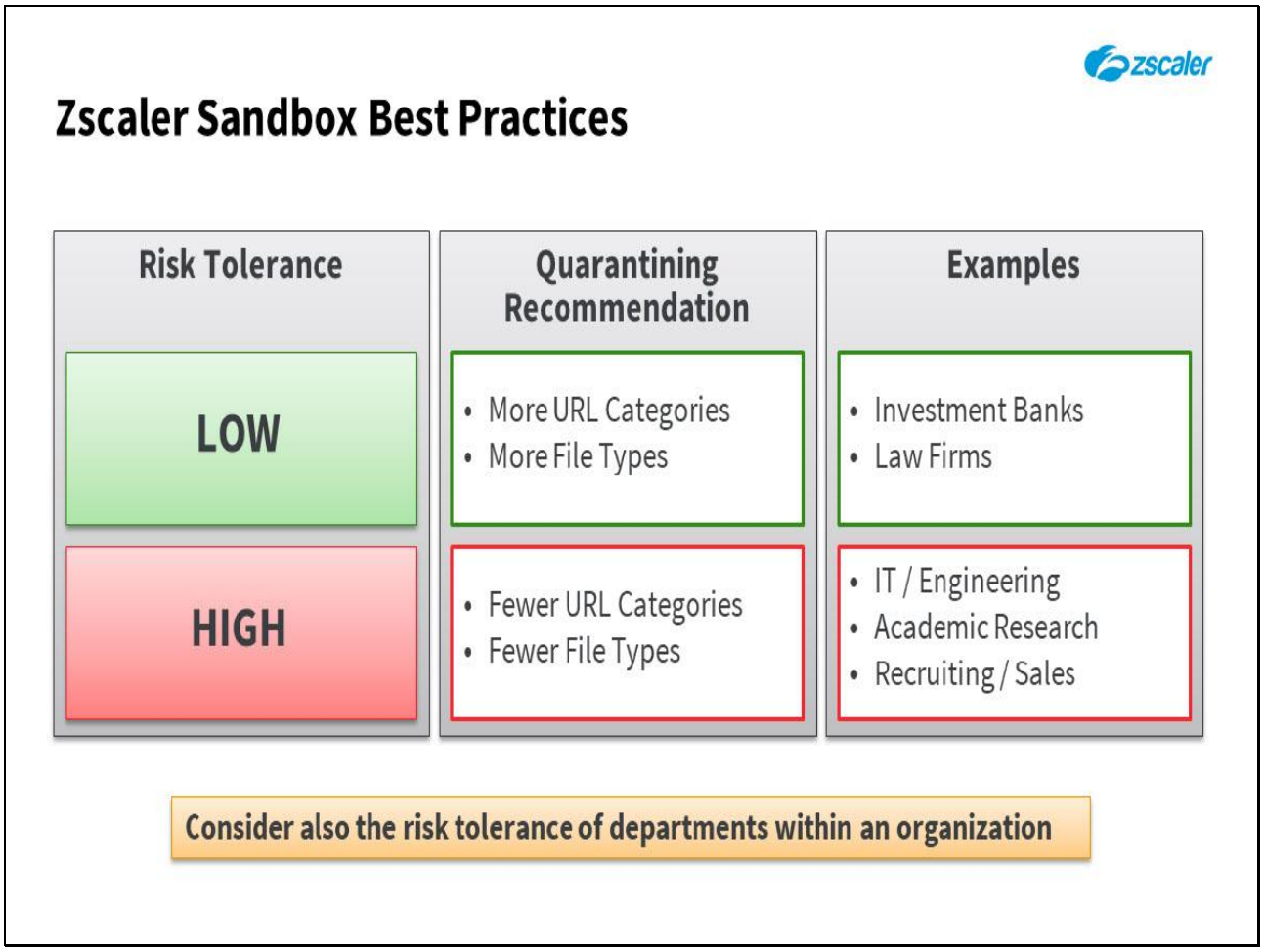
Slide 52 - Zscaler Sandbox Best Practices



Slide notes

Other organizations have a high tolerance for risk (such as IT or Engineering groups, Academic Research organizations, Recruiting or Sales organizations). These customers can probably get away with analyzing fewer URL categories and file types.

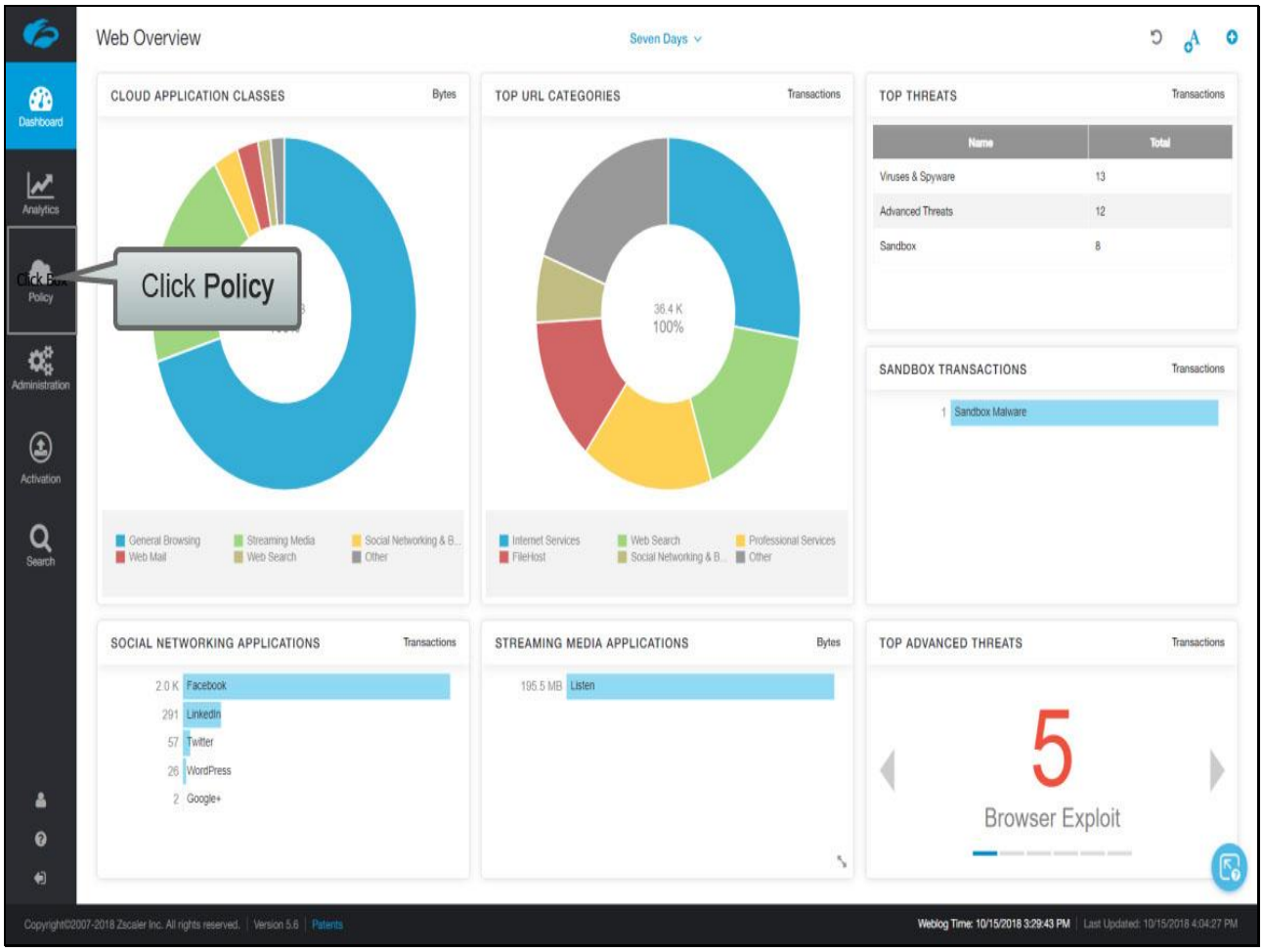
Slide 53 - Zscaler Sandbox Best Practices



Slide notes

Note that the tolerance for risk may well not be consistent throughout an organization, and the Sandbox configuration allows for customized rules per-user group, per-department, or even per-location.

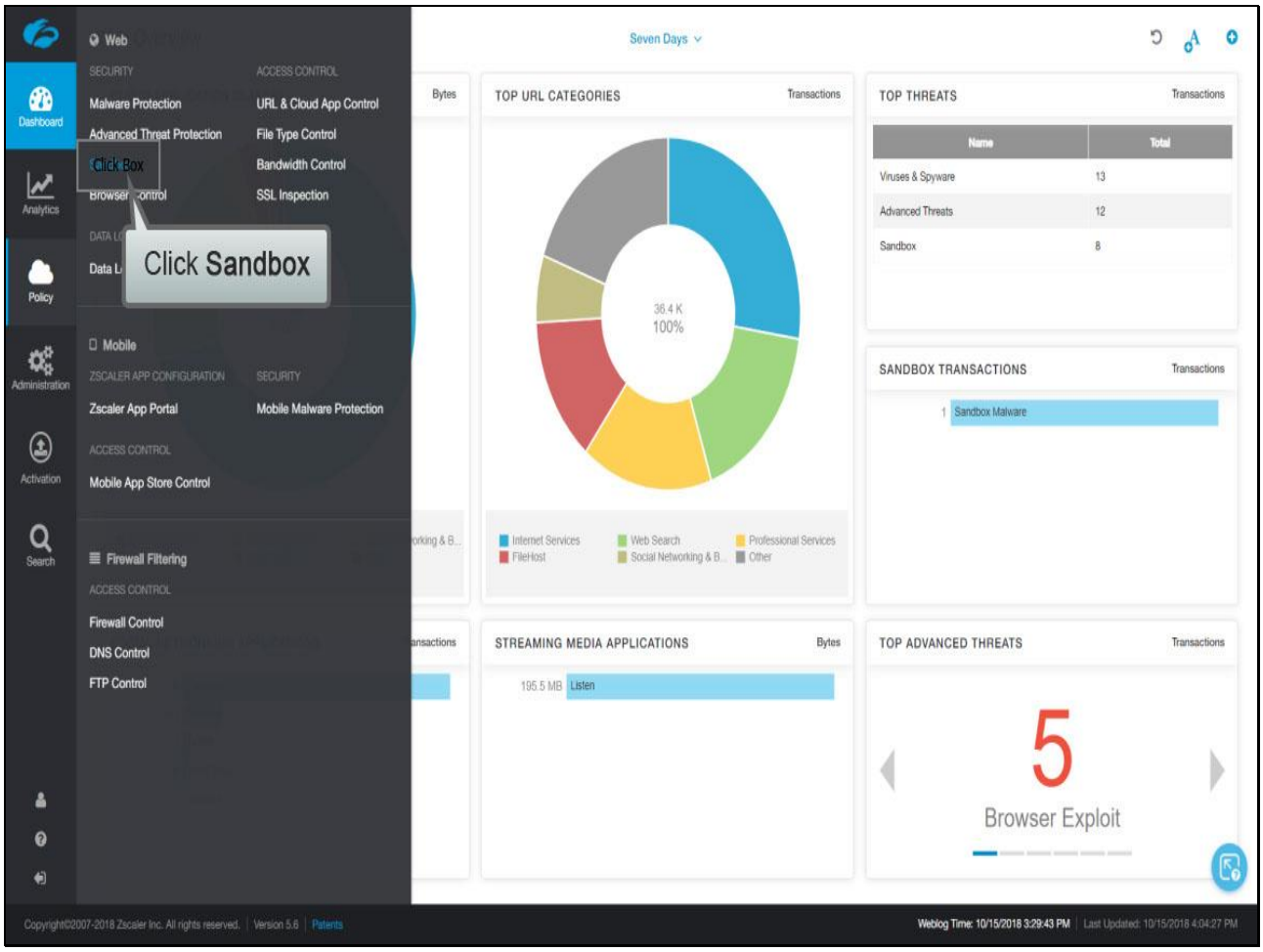
Slide 54 - Slide 54



Slide notes

To access the 'Sandbox' policy settings, click 'Policy', …

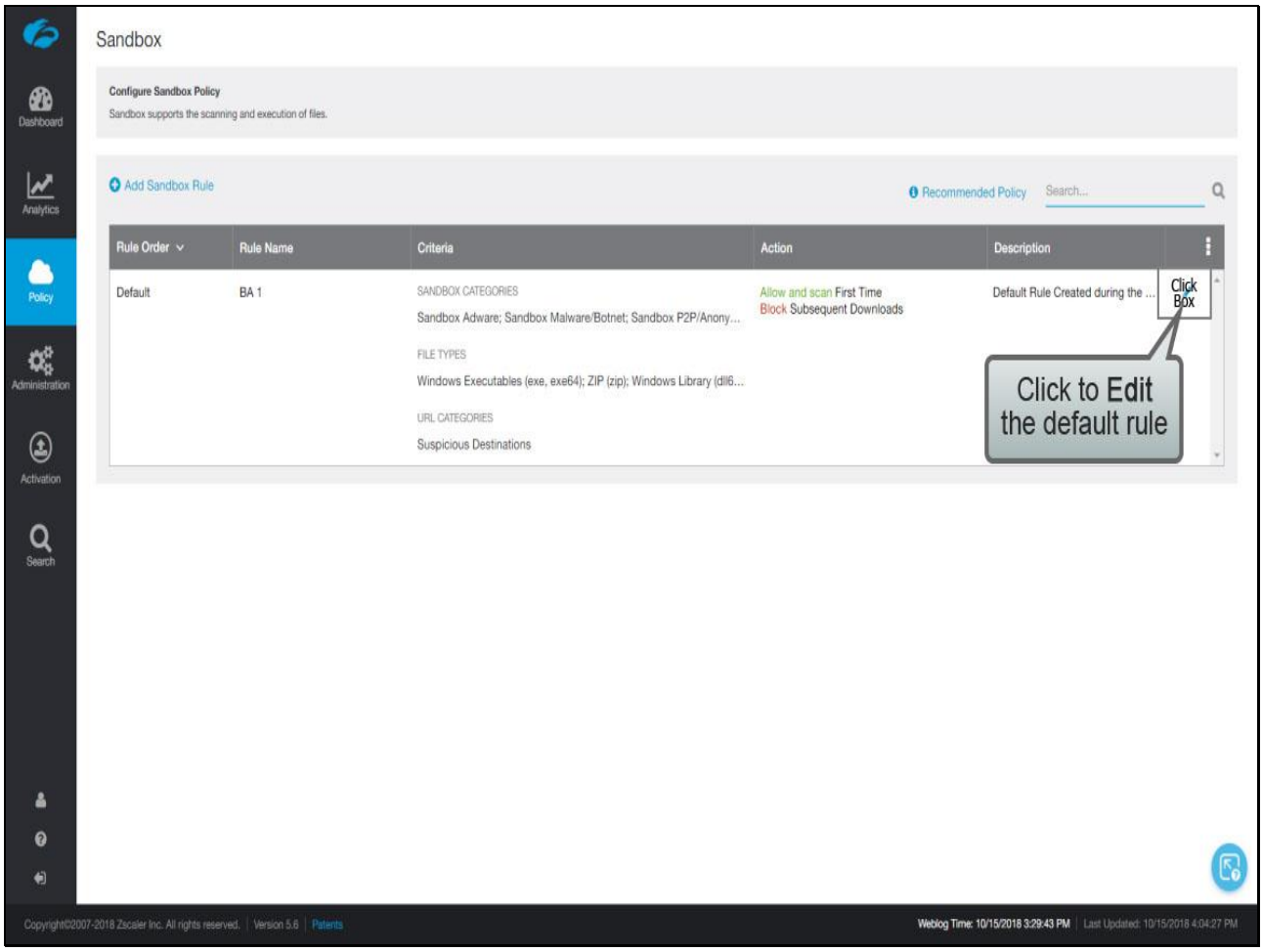
Slide 55 - Slide 55



Slide notes

…then from the ‘Web’ section of the ‘Policy’ menu, under the ‘SECURITY’ heading, click ‘Sandbox’.

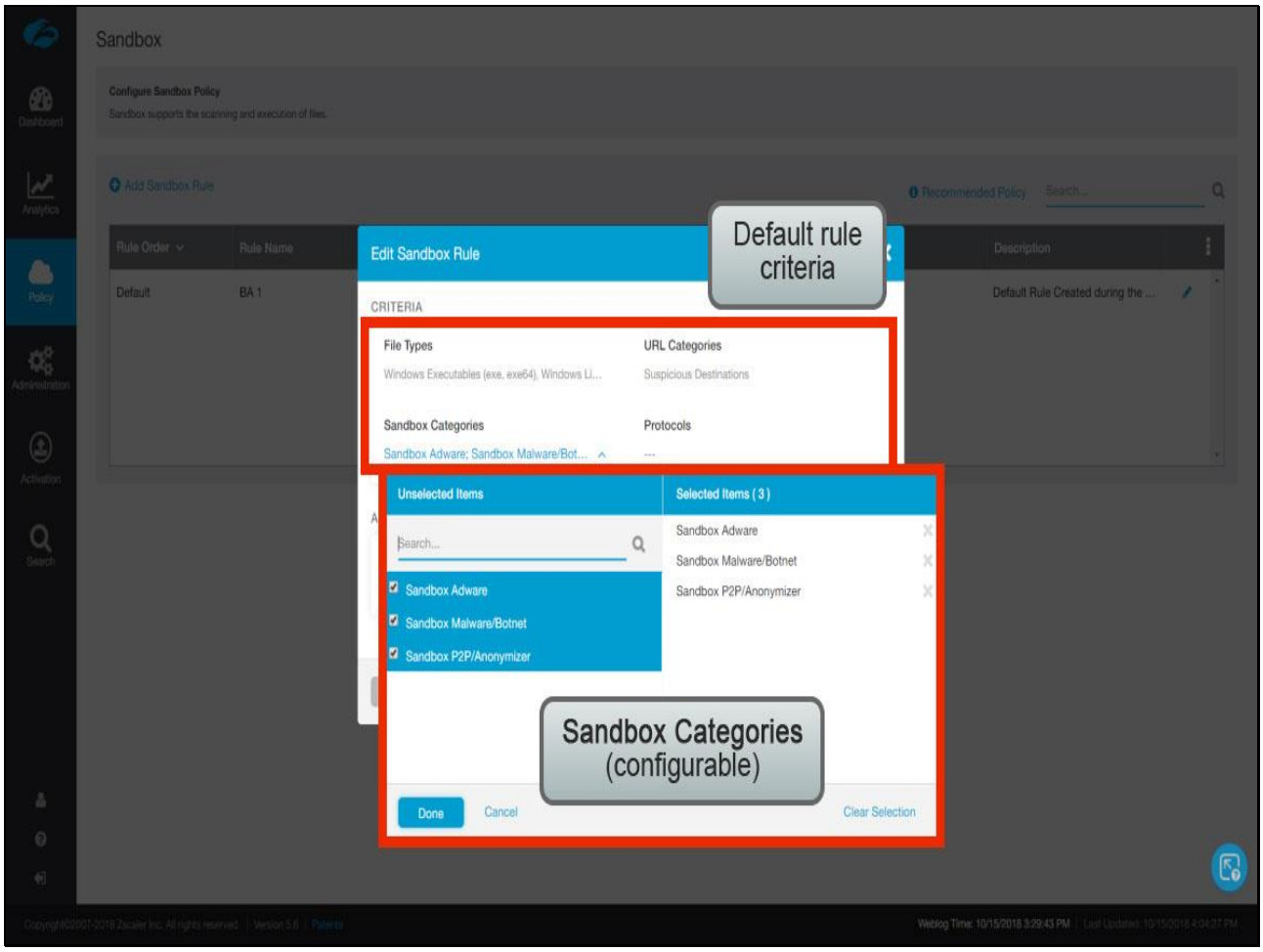
Slide 56 - Slide 56



Slide notes

There is a default Sandbox policy rule, click to edit it, …

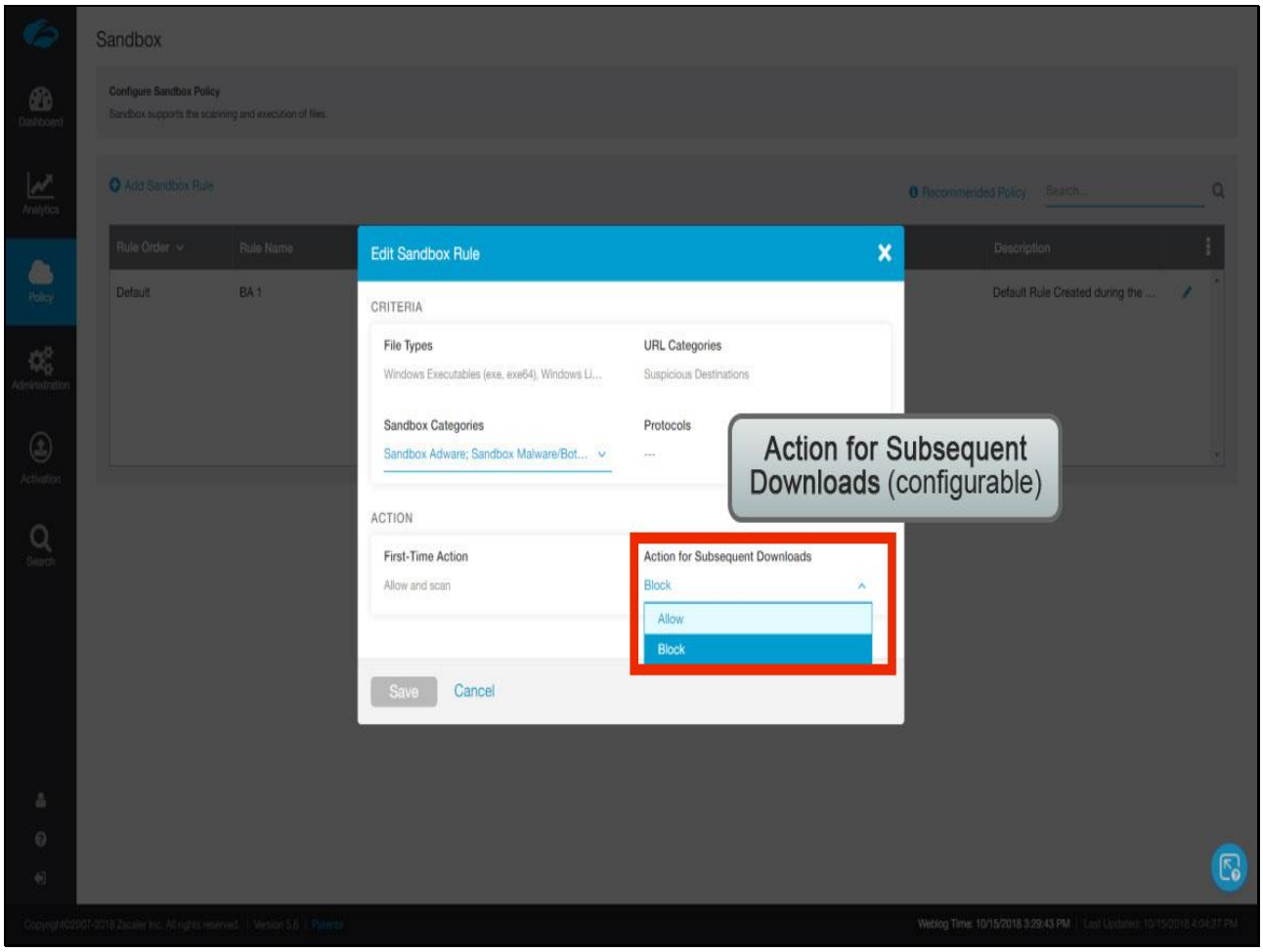
Slide 57 - Slide 57



Slide notes

…this policy is configured by default, to analyze suspicious Windows executable files (.exe) and dynamic link libraries (.dll) of traffic from URLs in suspicious URL categories. By default, the three ‘Sandbox Categories’ (‘Sandbox Adware’, ‘Sandbox Malware/Botnet’ and ‘Sandbox P2P/Anonymizer’) are enabled for analysis, although you can disable them if you choose.

Slide 58 - Slide 58

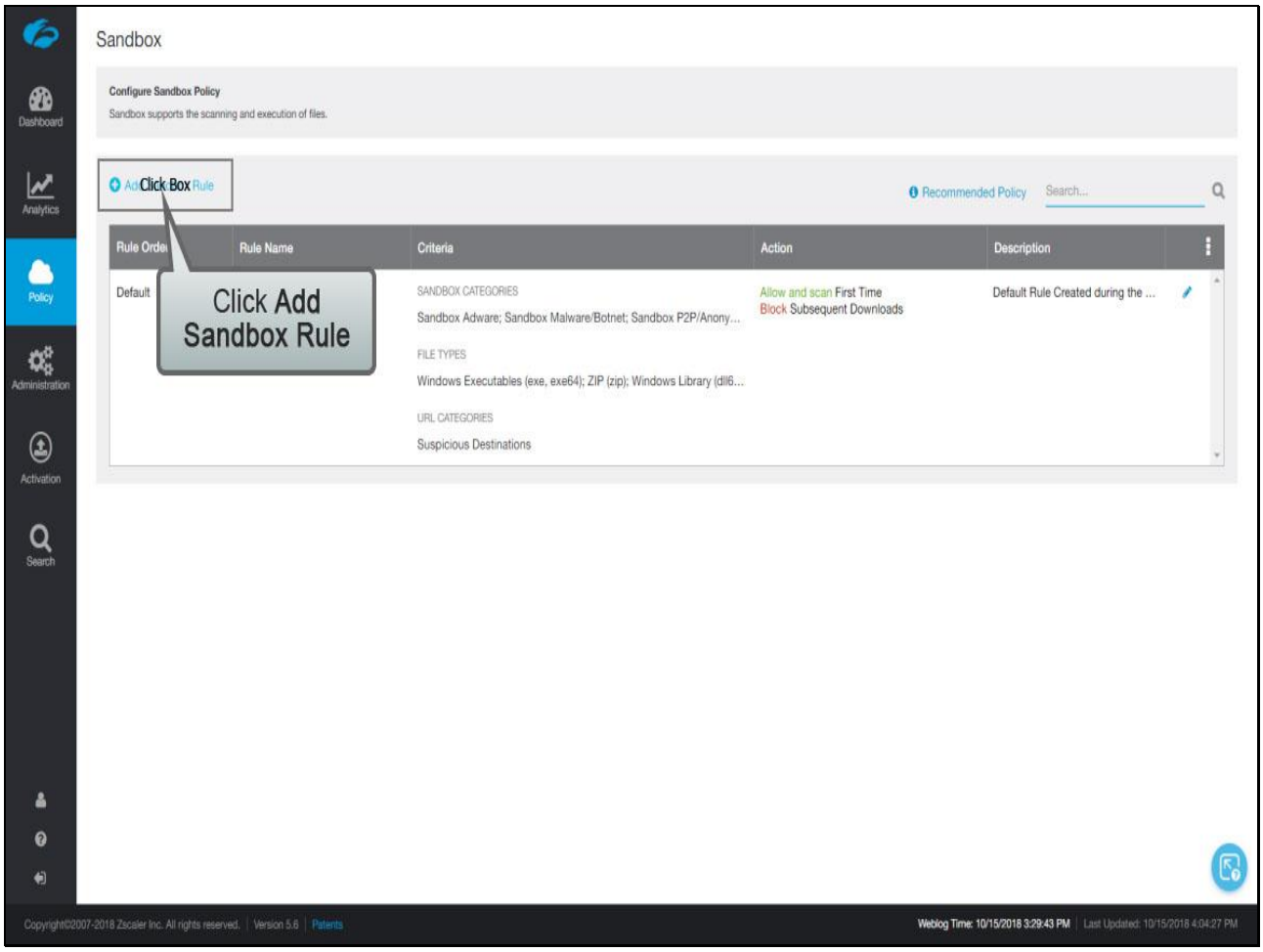


Slide notes

In most case the Zscaler service will have seen a file before and it will be examined with no delay to the user. However, if it is a new file and appears suspicious, Zscaler allows the download to proceed but will take the file and execute it in a sandbox to see what it does. The 'Action for Subsequent Downloads' is set by default to 'Block', although the 'Allow' option can be selected instead if you choose.

If you change the default rule, be sure to save and activate it!

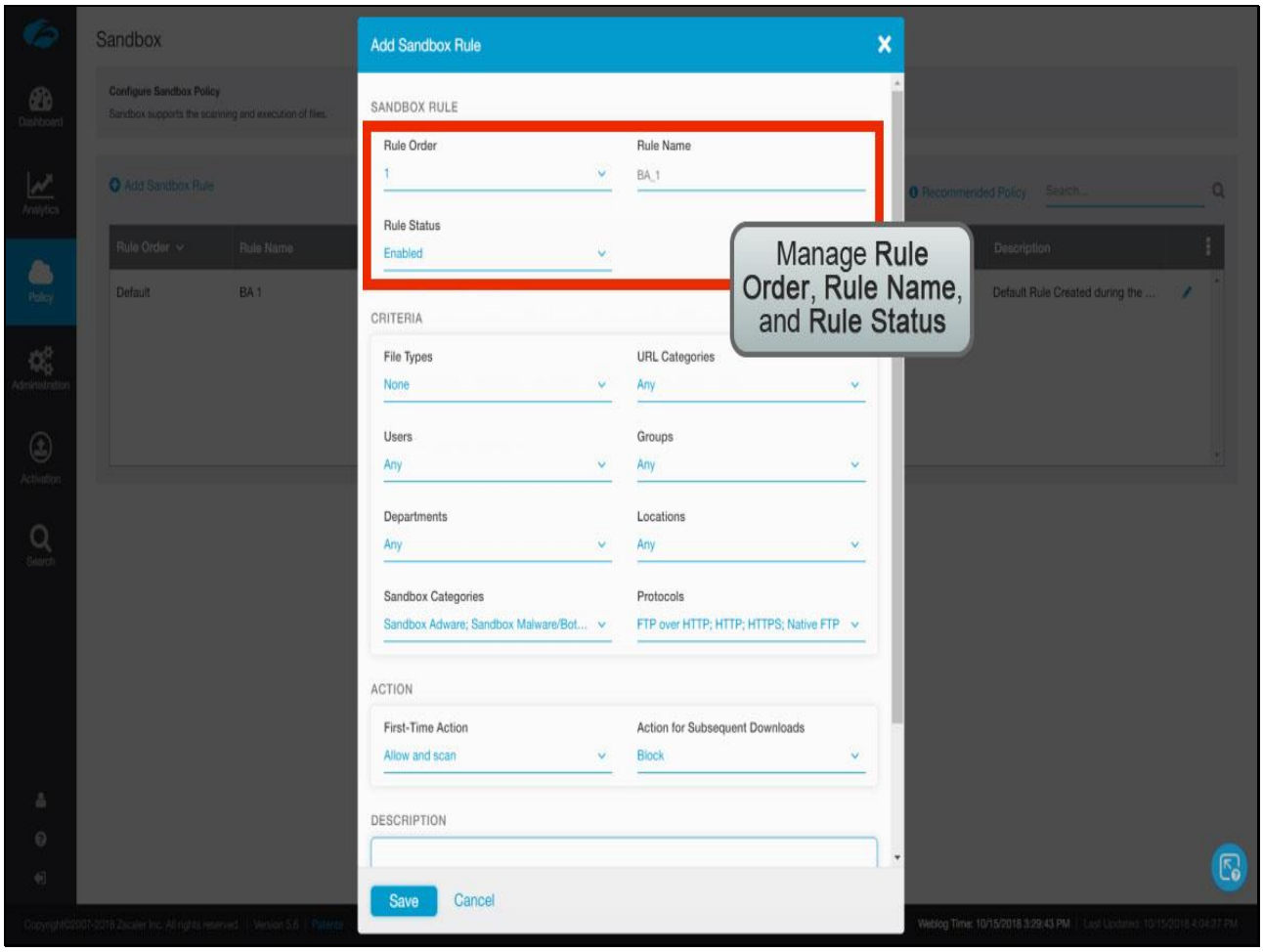
Slide 59 - Slide 59



Slide notes

To add a new ‘Sandbox’ Policy rule, click on the ‘Add Sandbox Rule’ link.

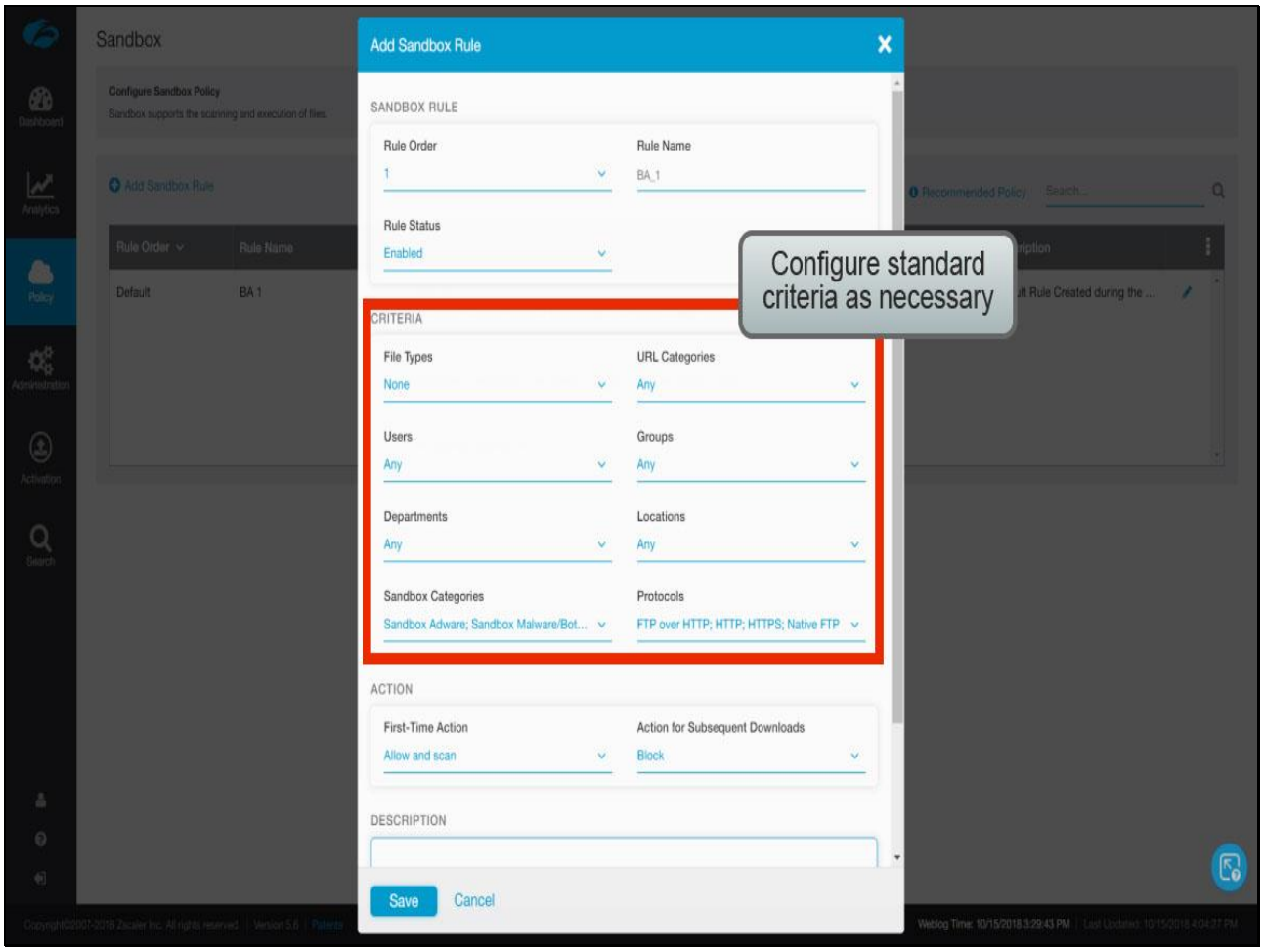
Slide 60 - Slide 60



Slide notes

You must specify the ‘Rule Order’, ‘Rule Name’, and ‘Status’, remembering that rules are read from the top down, and evaluation stops at the first match.

Slide 61 - Slide 61



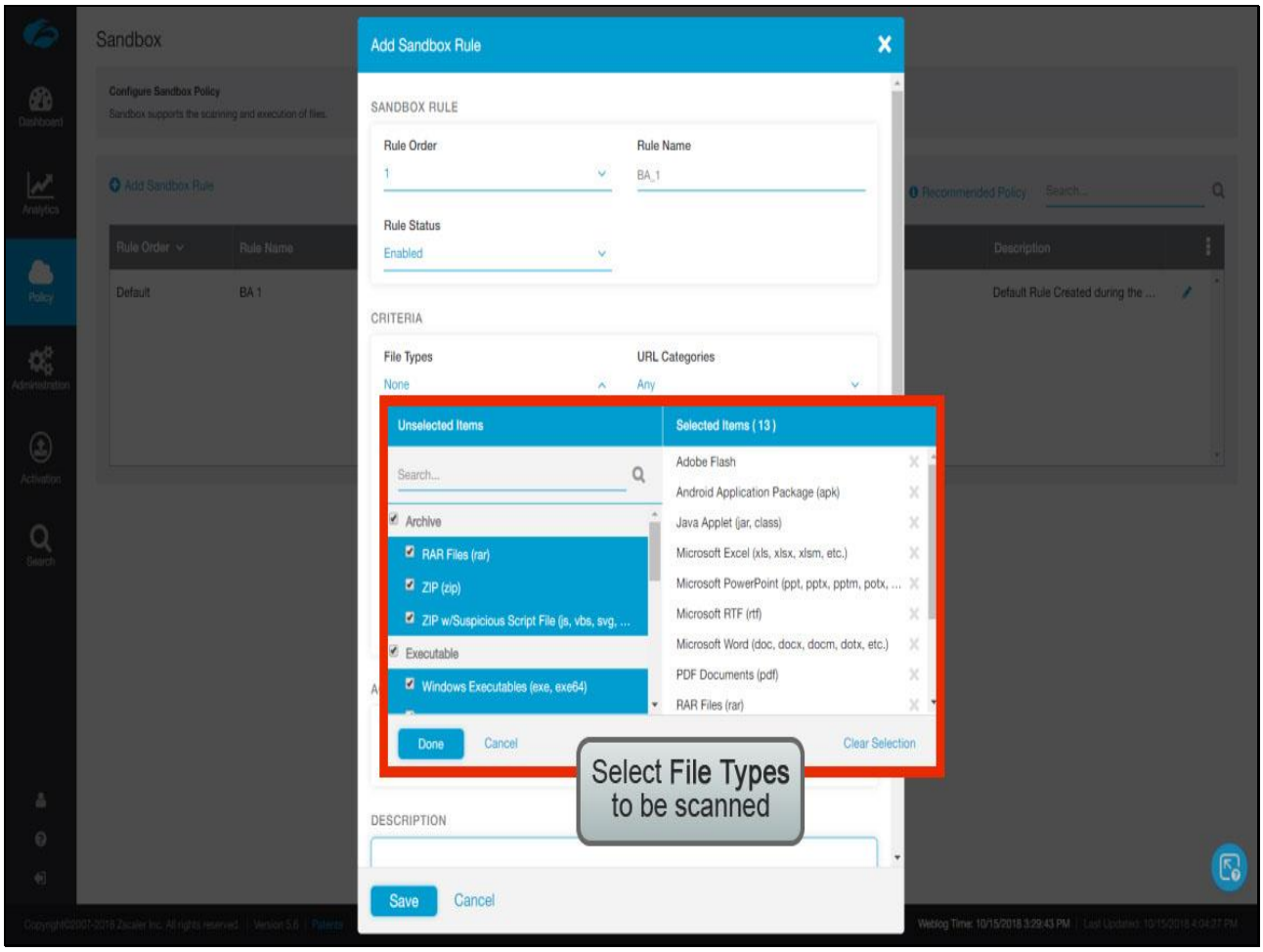
Slide notes

When adding a new 'Sandbox' rule, you can be as general or as specific as you need with the standard target criteria to target the rule based on any combination of:

- 'URL Categories';
- 'Users';
- 'Groups';
- 'Departments';
- 'Locations',
- Or 'Protocols'.

Note that we will talk about the 'URL Categories' shortly, when looking at the 'URL & Cloud App Control' Policy.

Slide 62 - Slide 62



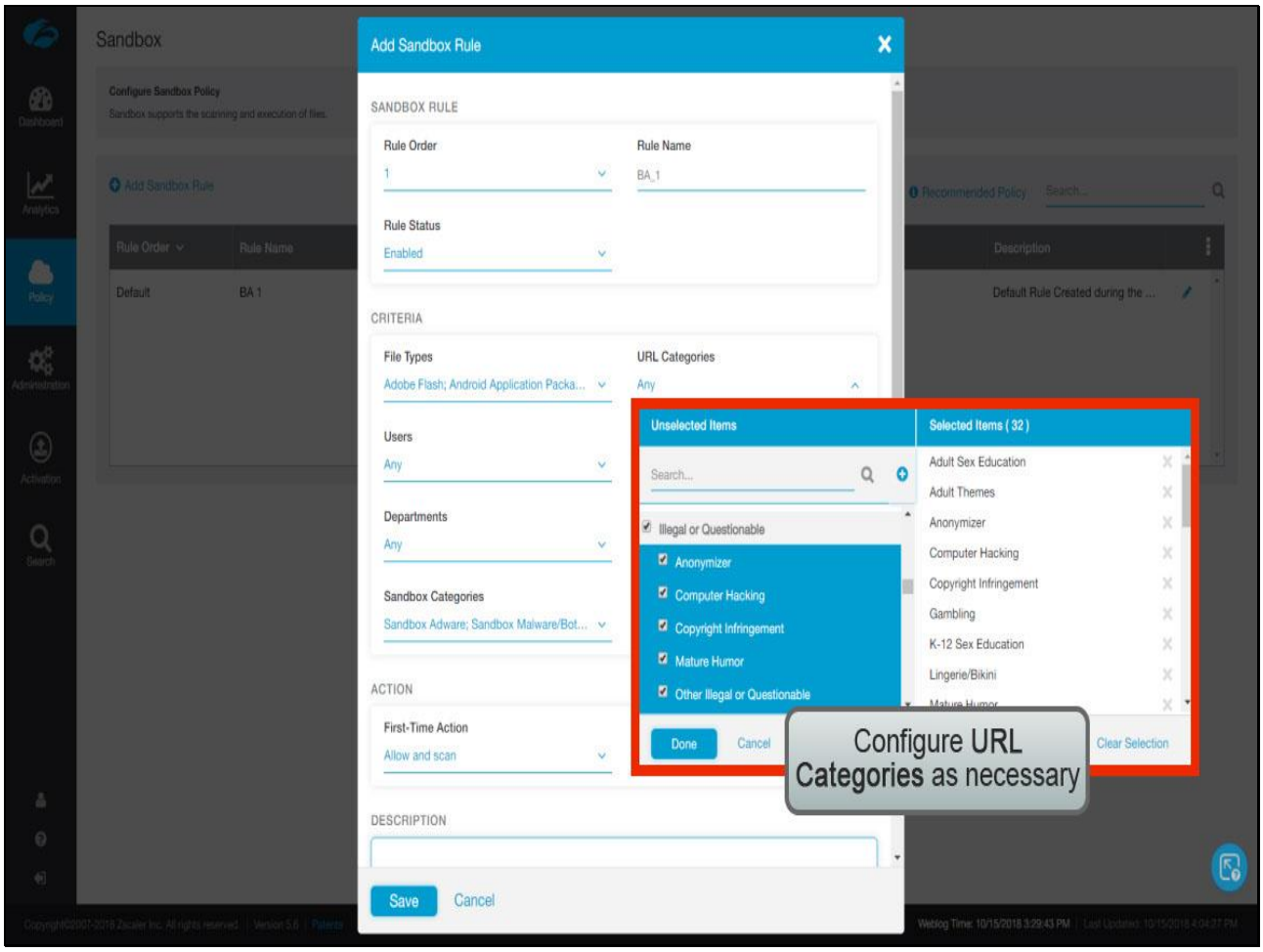
Slide notes

With a basic subscription, the only file types that can be selected for scanning are executables, and .DLL files, up to 2MB in size.

With the Advanced Cloud Sandbox subscription, there is no file size restriction, and the files that can be scanned include:

- 'Archive' files (.RAR, .ZIP, and .ZIP with suspicious Script Files);
- 'Executables' (including Windows library files);
- 'Microsoft Office' files (with all the Excel, PowerPoint, RTF and Word file formats, including the macro enabled versions of these formats);
- 'Mobile' files, specifically Android application packages (.APKs);
- 'Other Documents', which includes .PDF documents;
- And 'Web Content' , such as Adobe Flash and Java applets.

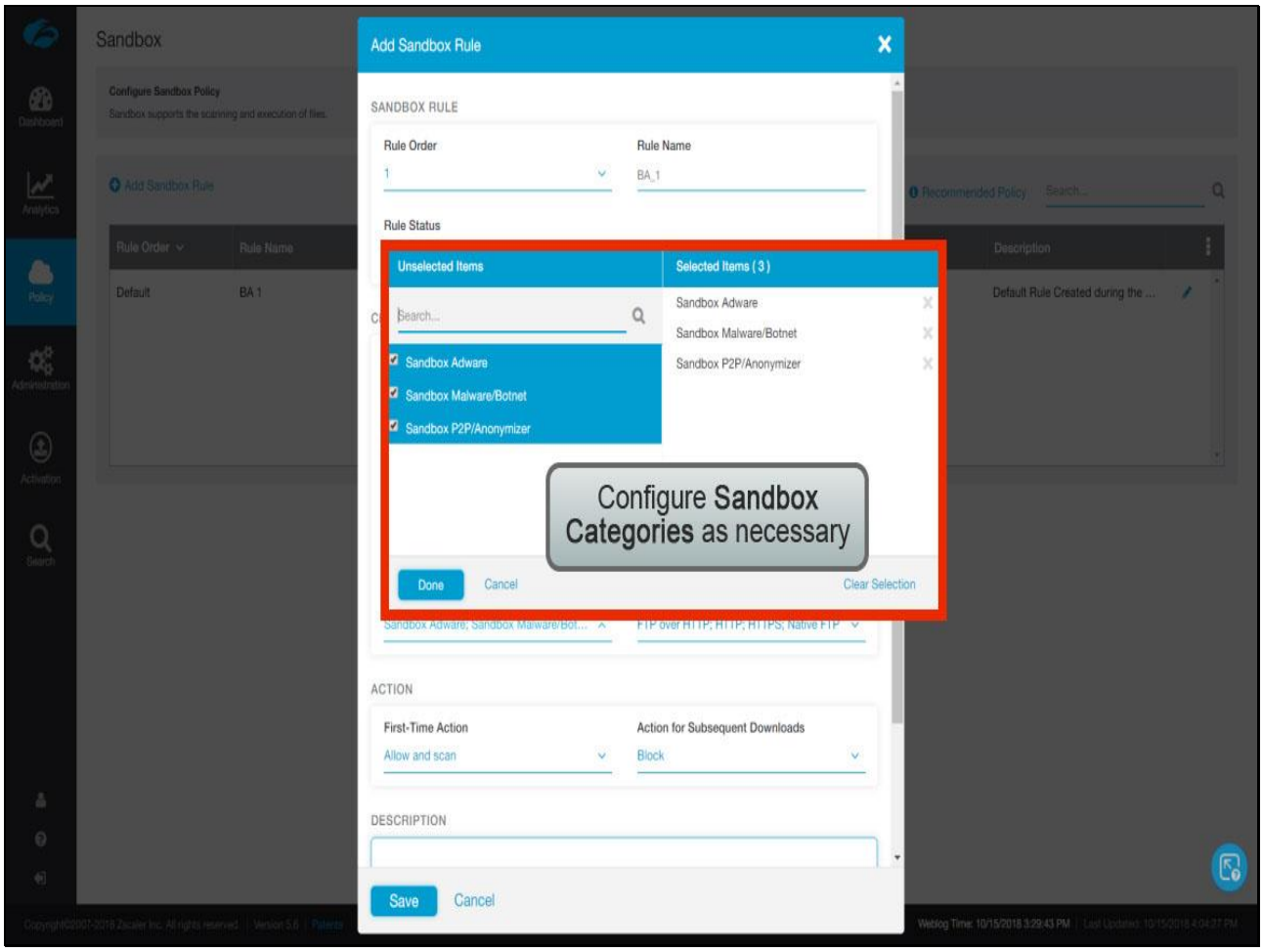
Slide 63 - Slide 63



Slide notes

Typically, you would target a rule against the ‘Legal Liability’ URL Categories, although you are free to select any appropriate categories.

Slide 64 - Slide 64

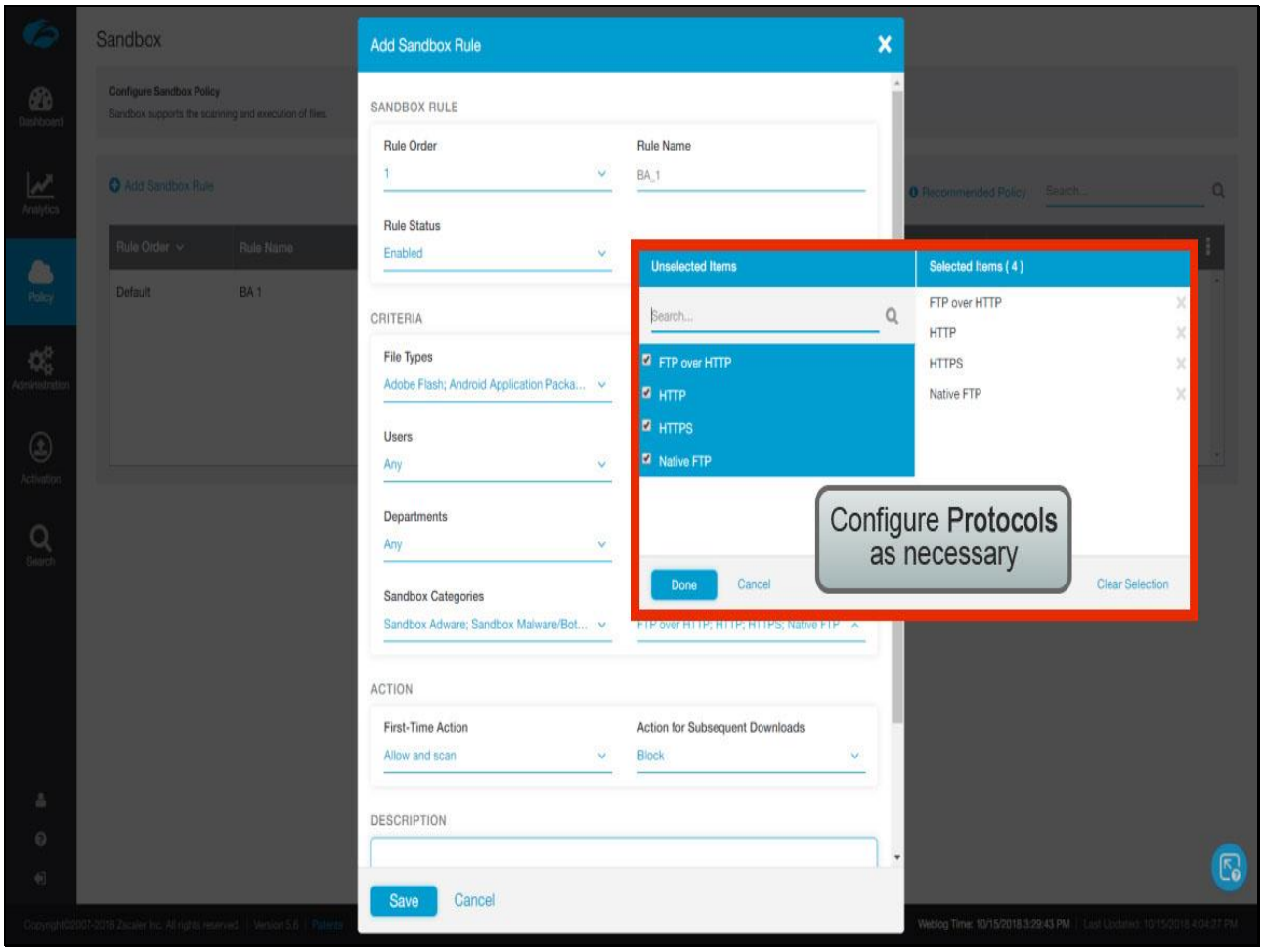


Slide notes

You can also target a rule against any combination of the three ‘Sandbox’ Categories:

- ‘Sandbox Adware’;
- ‘Sandbox Malware/Botnet’;
- Or ‘Sandbox P2P/Anonymizer’.

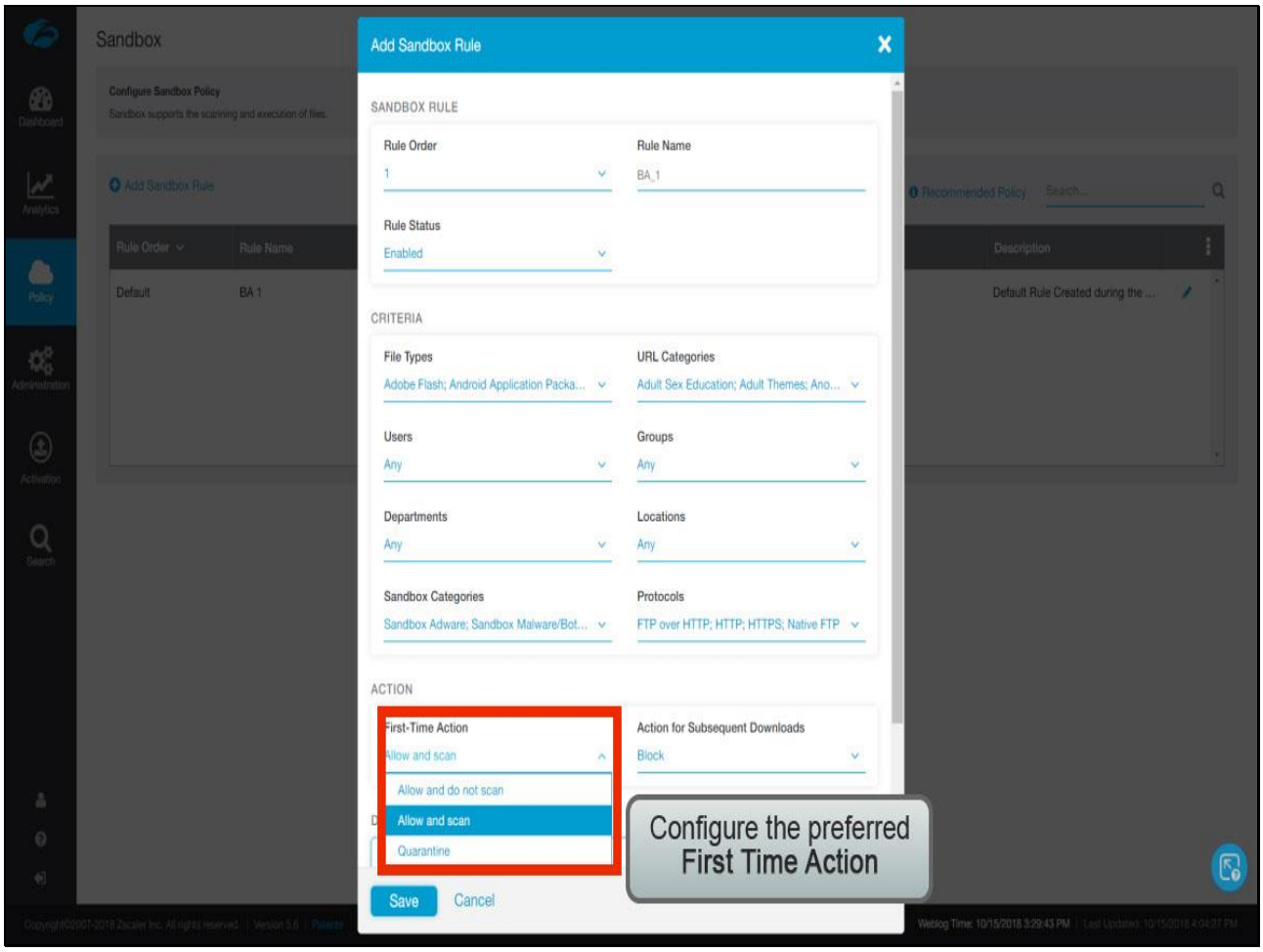
Slide 65 - Slide 65



Slide notes

You can specify the ‘Protocols’ the rule is to be applied to, any combination of; ‘FTP over HTTP’, ‘HTTP’, ‘HTTPS’, or ‘Native FTP’.

Slide 66 - Slide 66



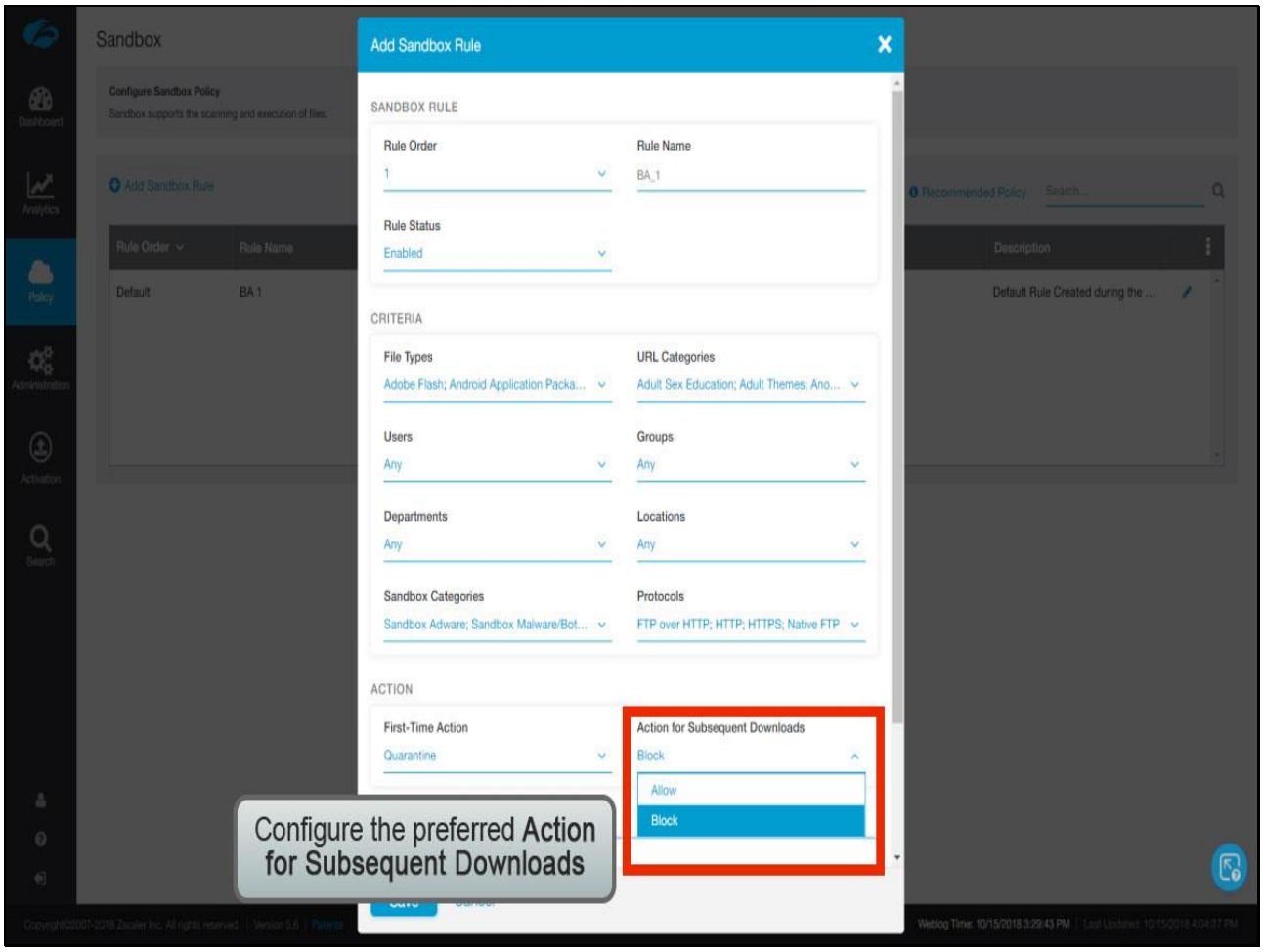
Slide notes

Specify the action to be taken when Zscaler sees a file for the first time, the options here being:

- ‘Allow and do not scan’;
- ‘Allow and scan’;
- Or ‘Quarantine’.

The decision to be made here is whether you want to make the user wait while Zscaler scans the file, the typical delay for scanning being less than 10 minutes. If you choose to quarantine the file, then while the file is being scanned the user will see a ‘Please Wait’ message. This message will be automatically refreshed at intervals while the file is ‘detonated’ in the Sandbox.

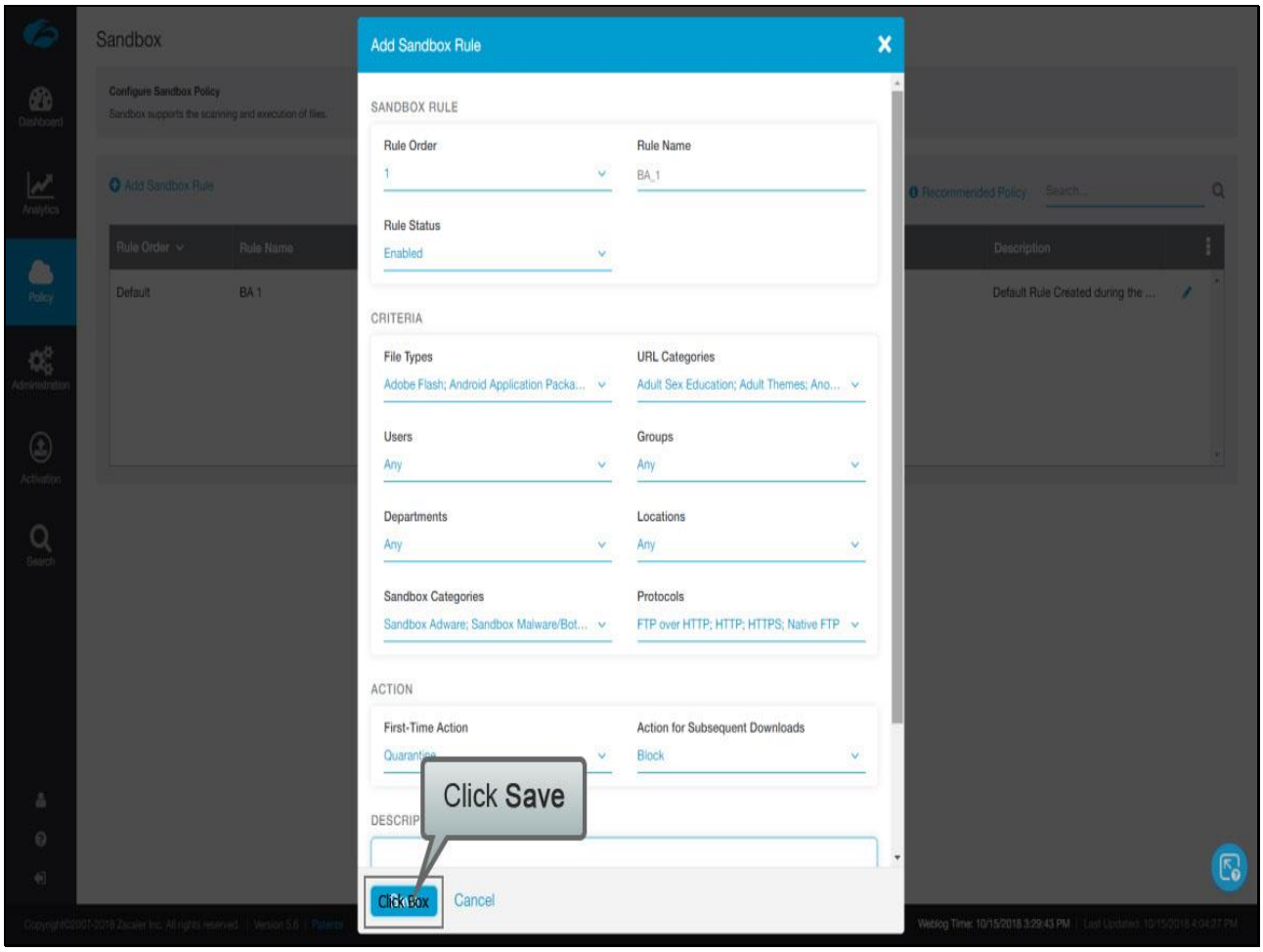
Slide 67 - Slide 67



Slide notes

Then specify what Zscaler should do on subsequent downloads of the file, whether to; ‘Block’, or ‘Allow’.

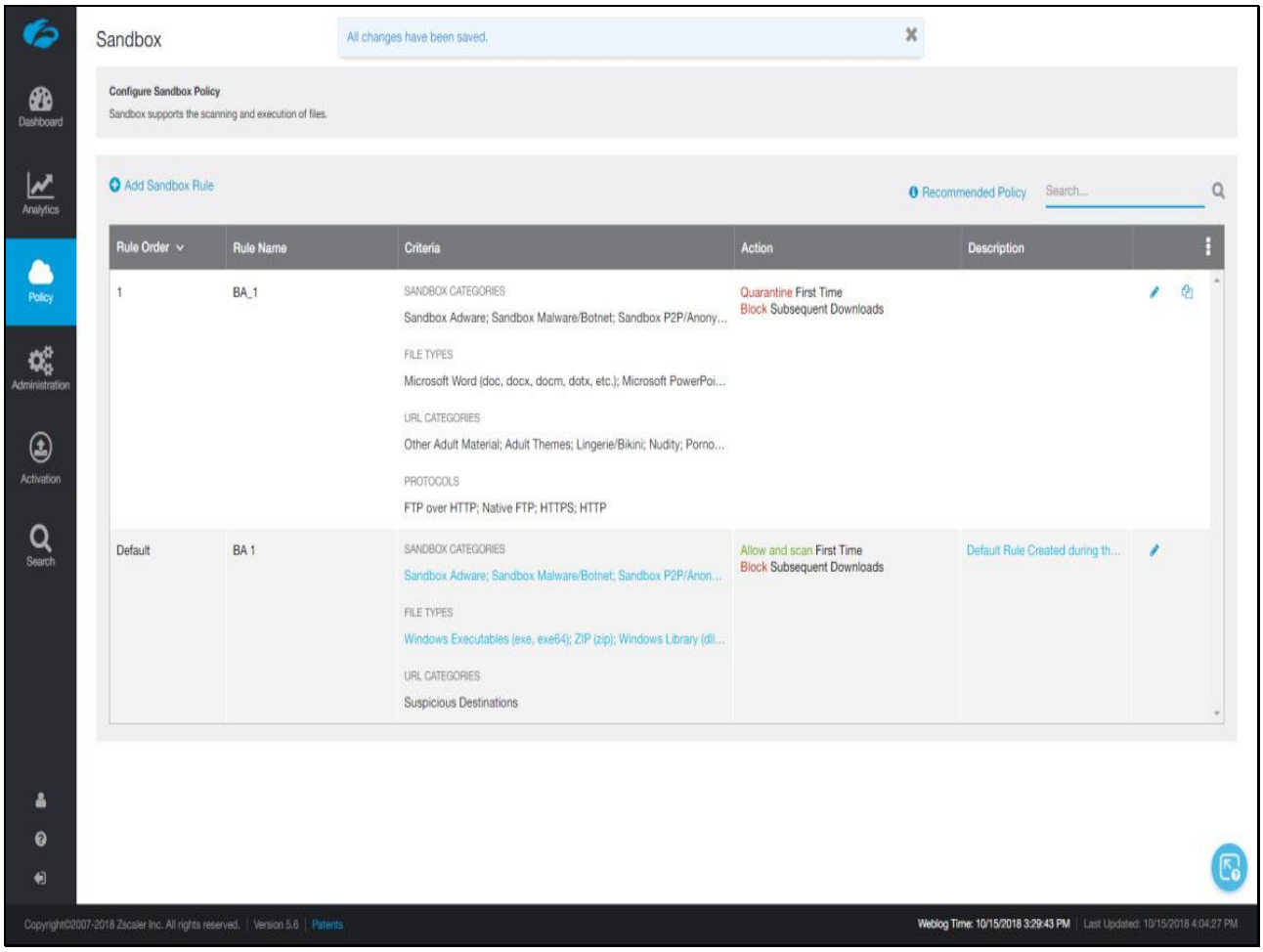
Slide 68 - Slide 68



Slide notes

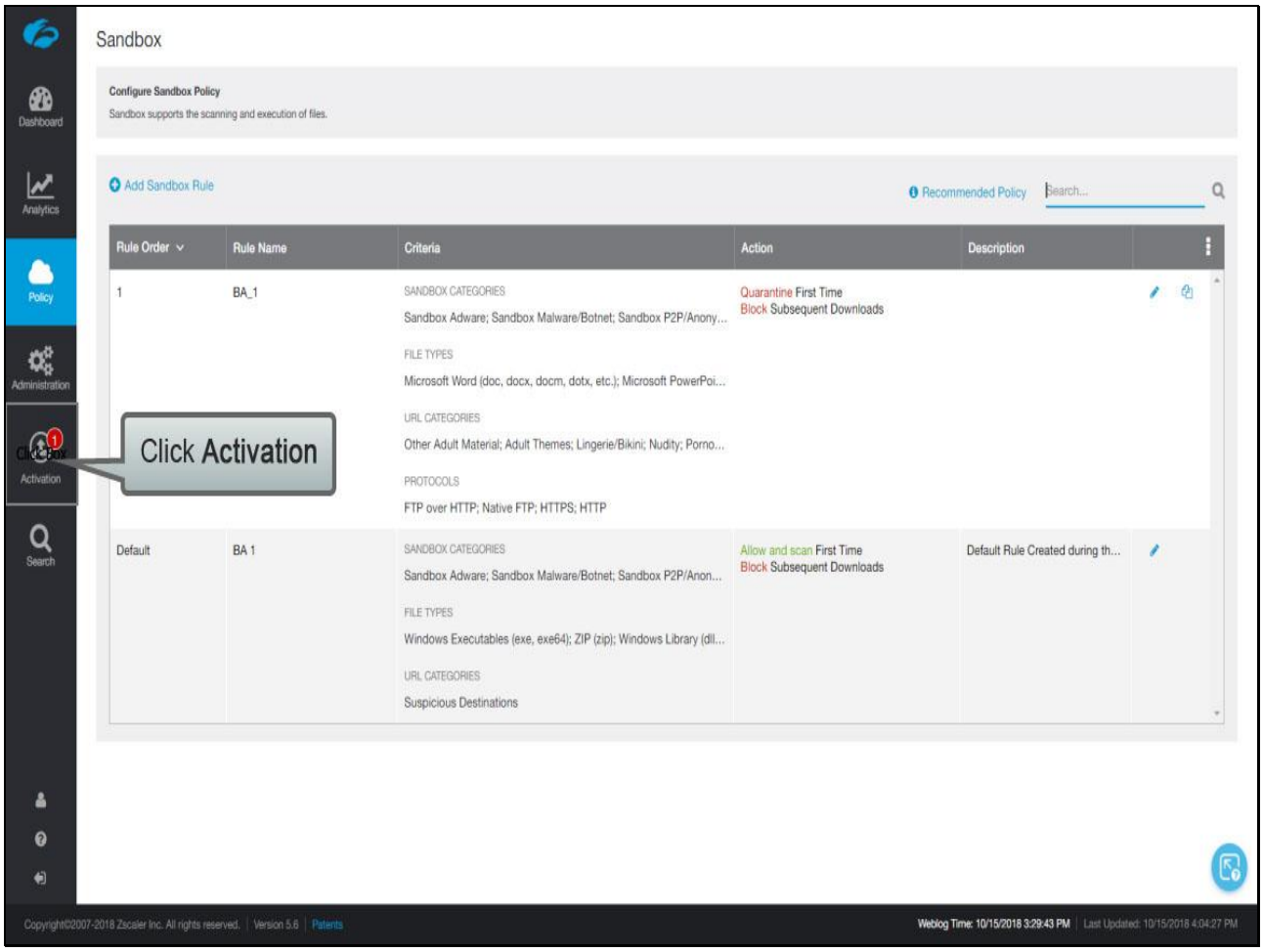
Having configured the Cloud Sandbox policy rule as necessary, click ‘Save’.

Slide 69 - Slide 69



Slide notes

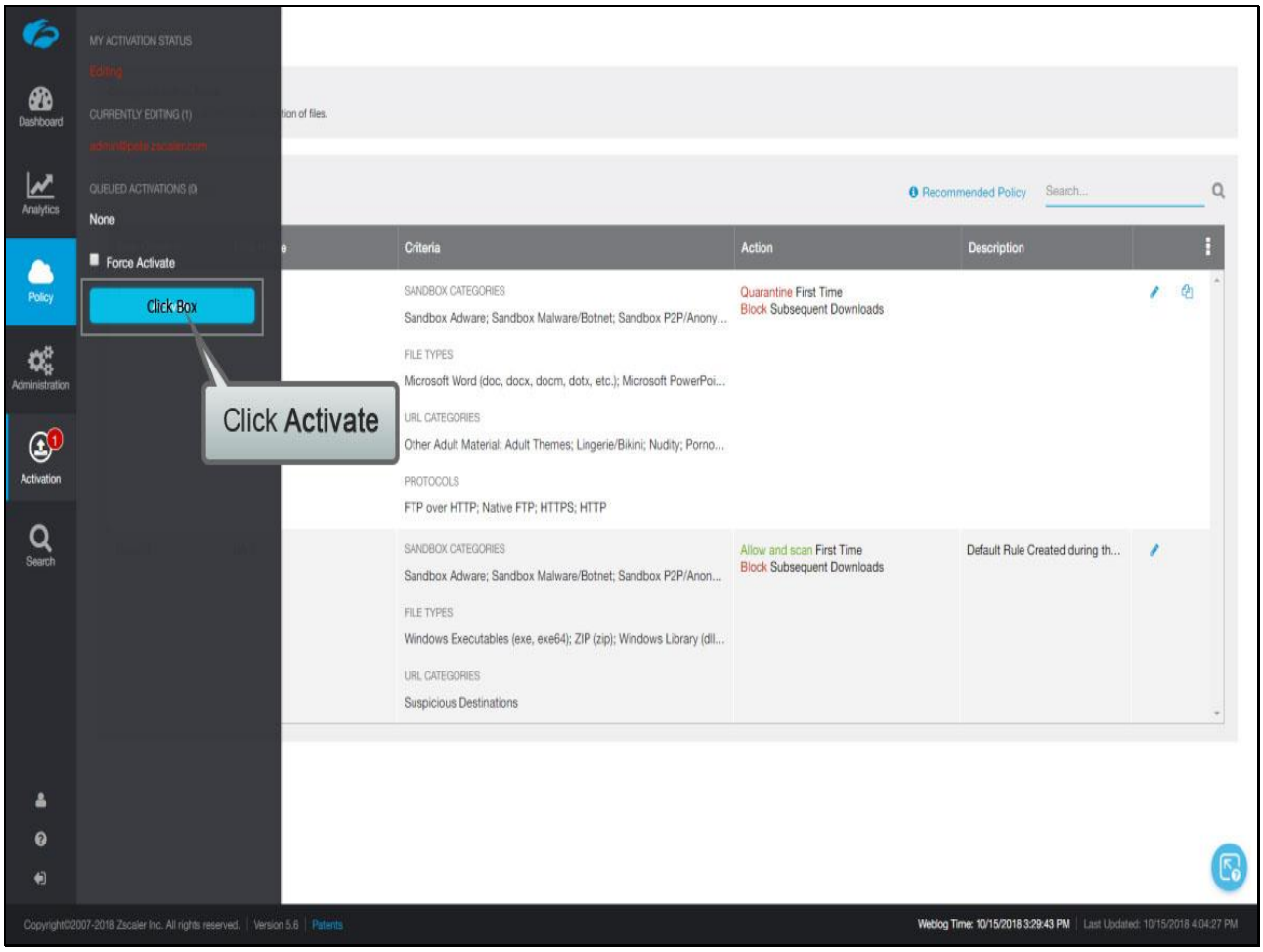
Slide 70 - Slide 70



Slide notes

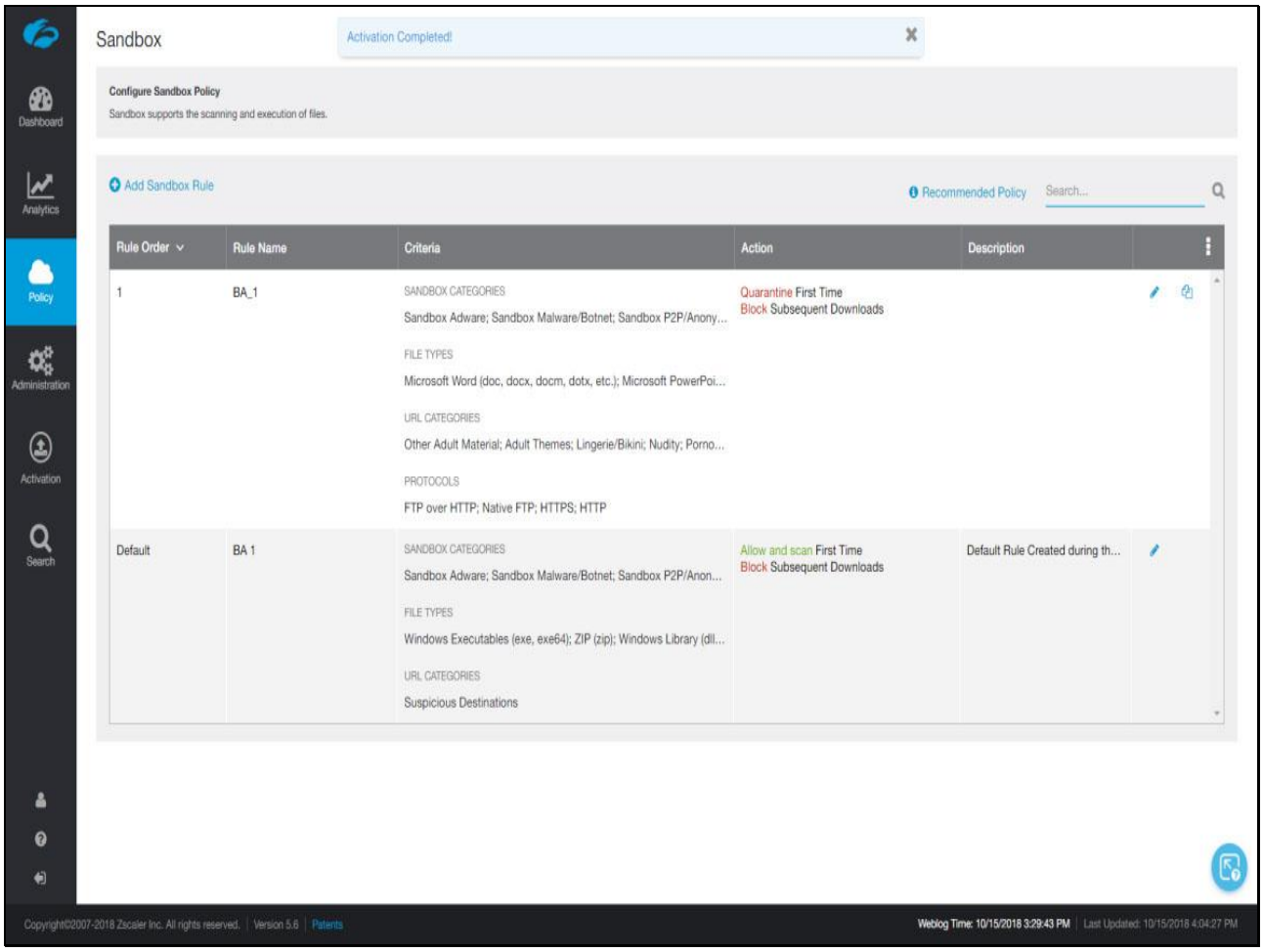
…and ‘Activate’ your changes.

Slide 71 - Slide 71



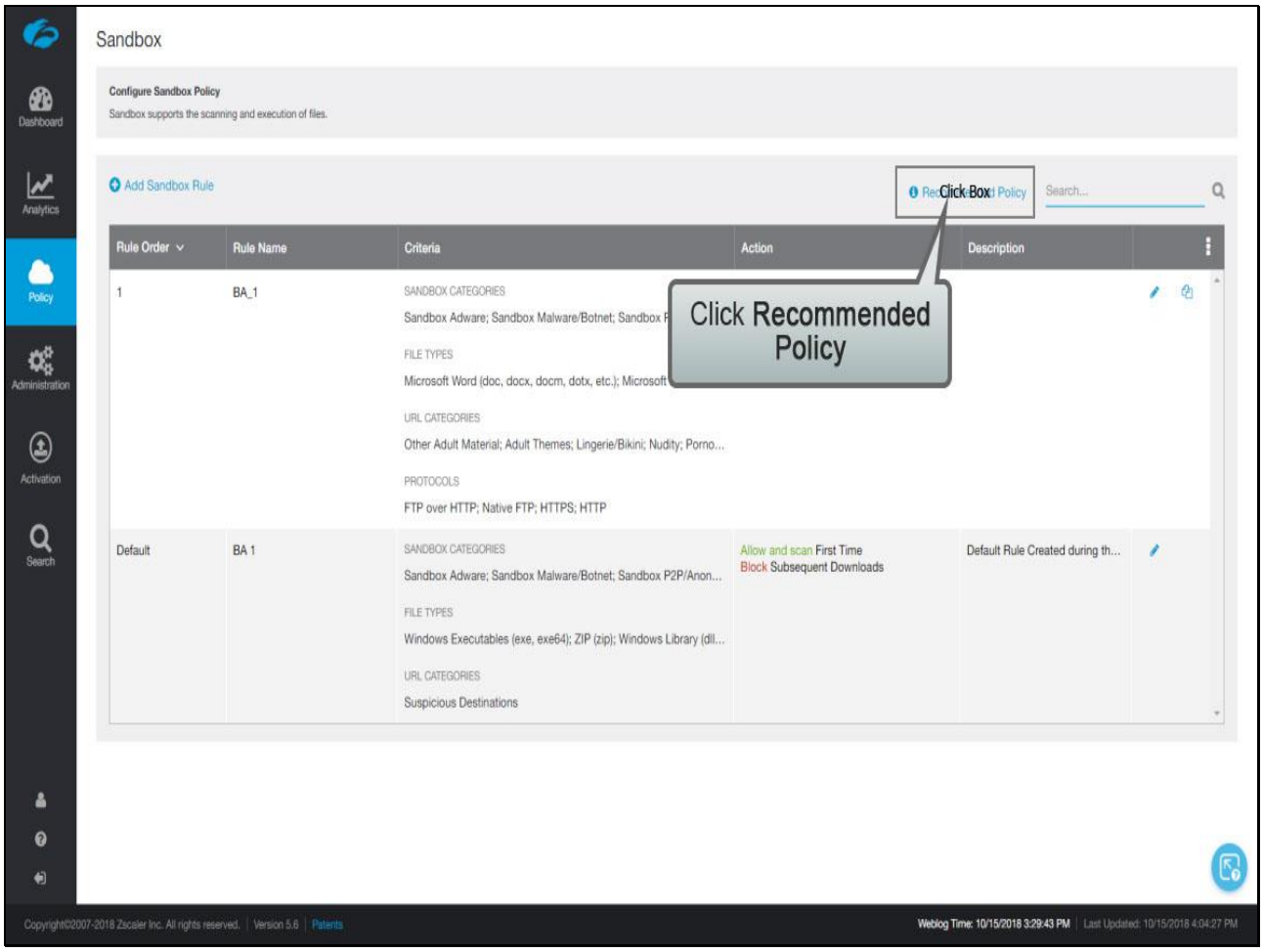
Slide notes

Slide 72 - Slide 72



Slide notes

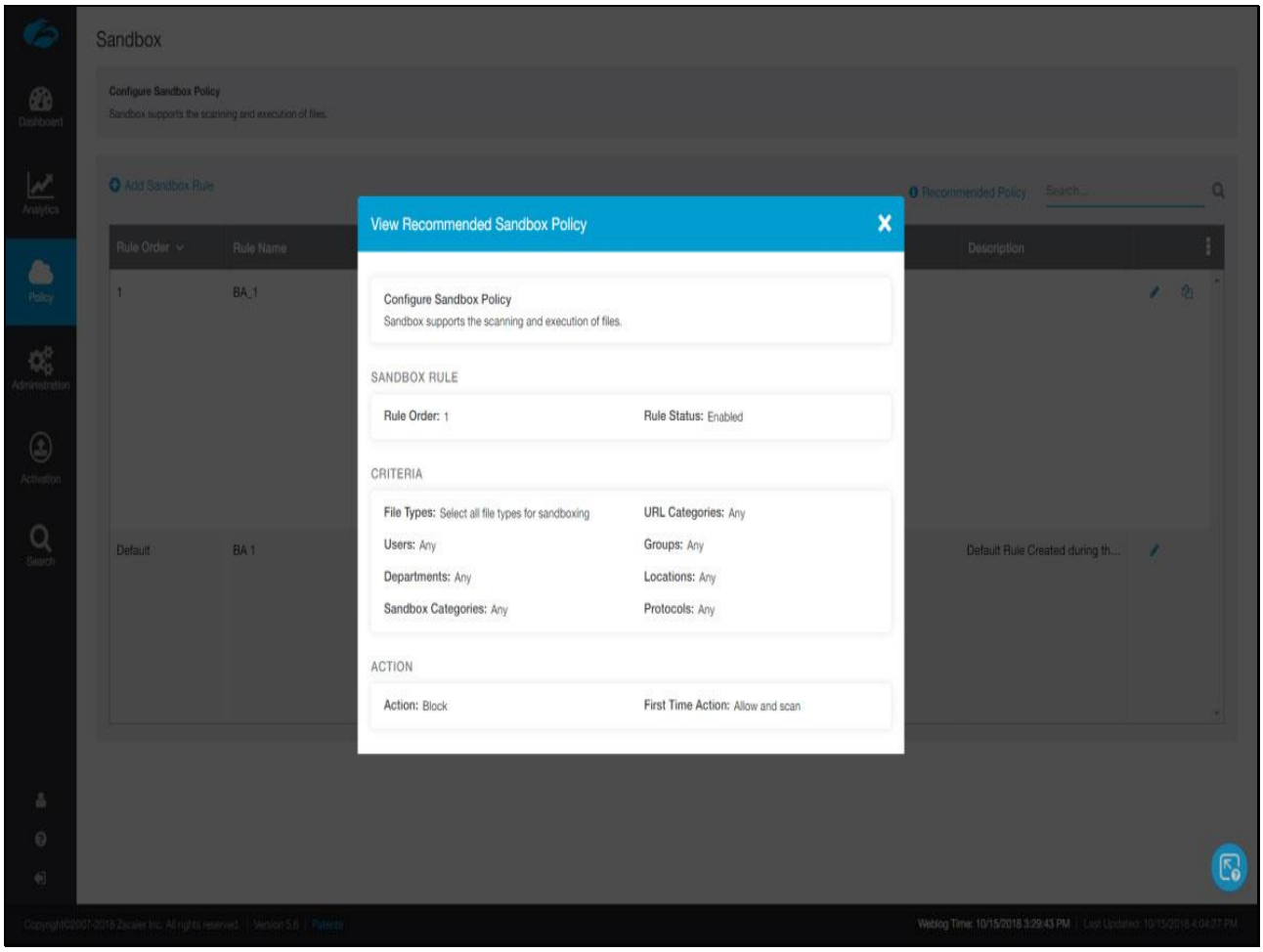
Slide 73 - Slide 73



Slide notes

To see Zscaler recommendations for configuring ‘Sandbox’ Policy settings, click the ‘Recommended Policy’ link.

Slide 74 - Slide 74

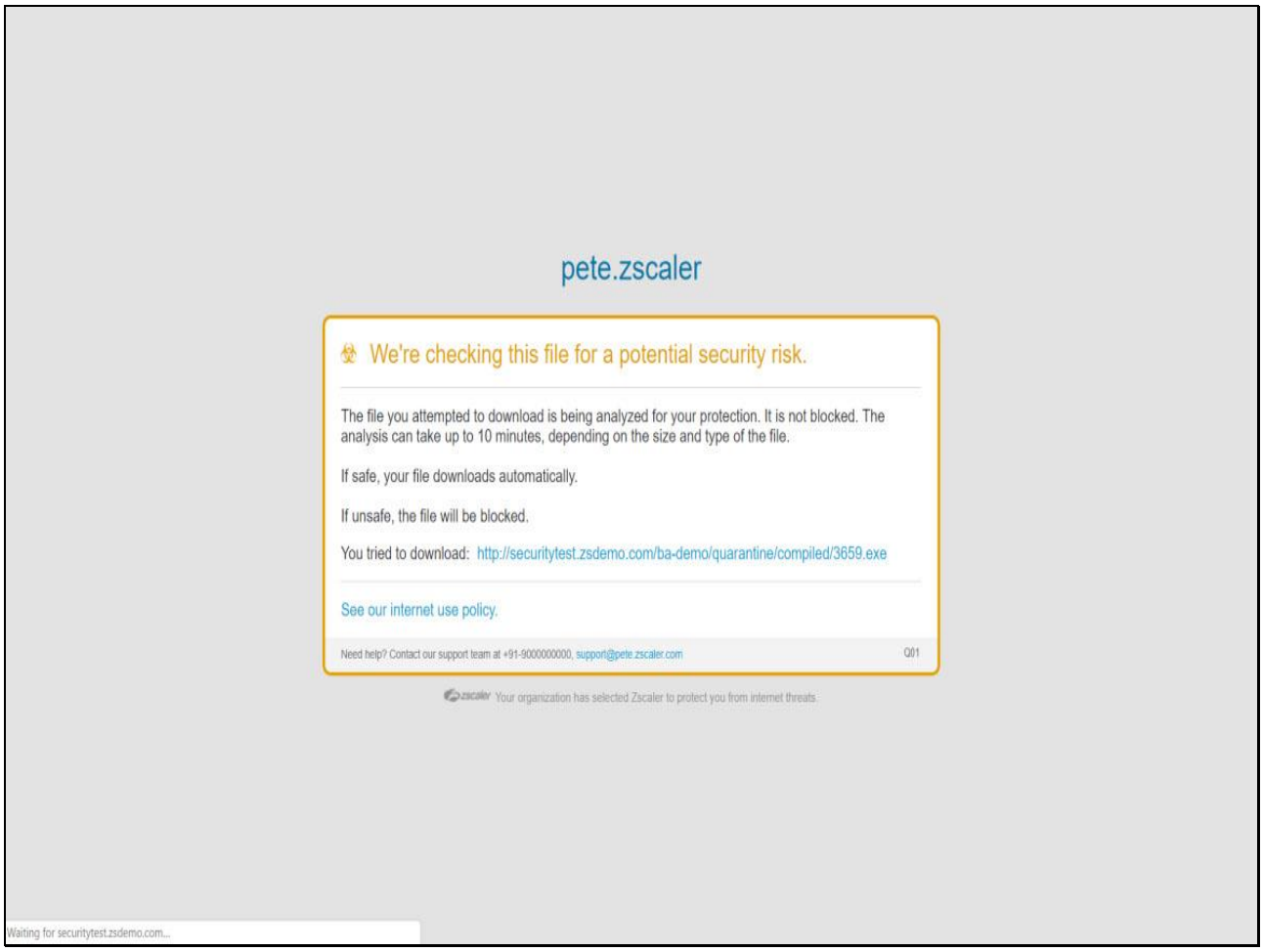


Slide notes

For the ‘Sandbox’ Policy Zscaler recommends that you:

- Analyze all ‘File Types’ of traffic from any ‘URL Categories’, that match any of the ‘Sandbox Categories’;
- That you ‘Block’ files known to contain Adware, Botnets & Malware, or Anonymizers or P2P clients;
- And that you ‘Allow and scan’ files seen for the first time.

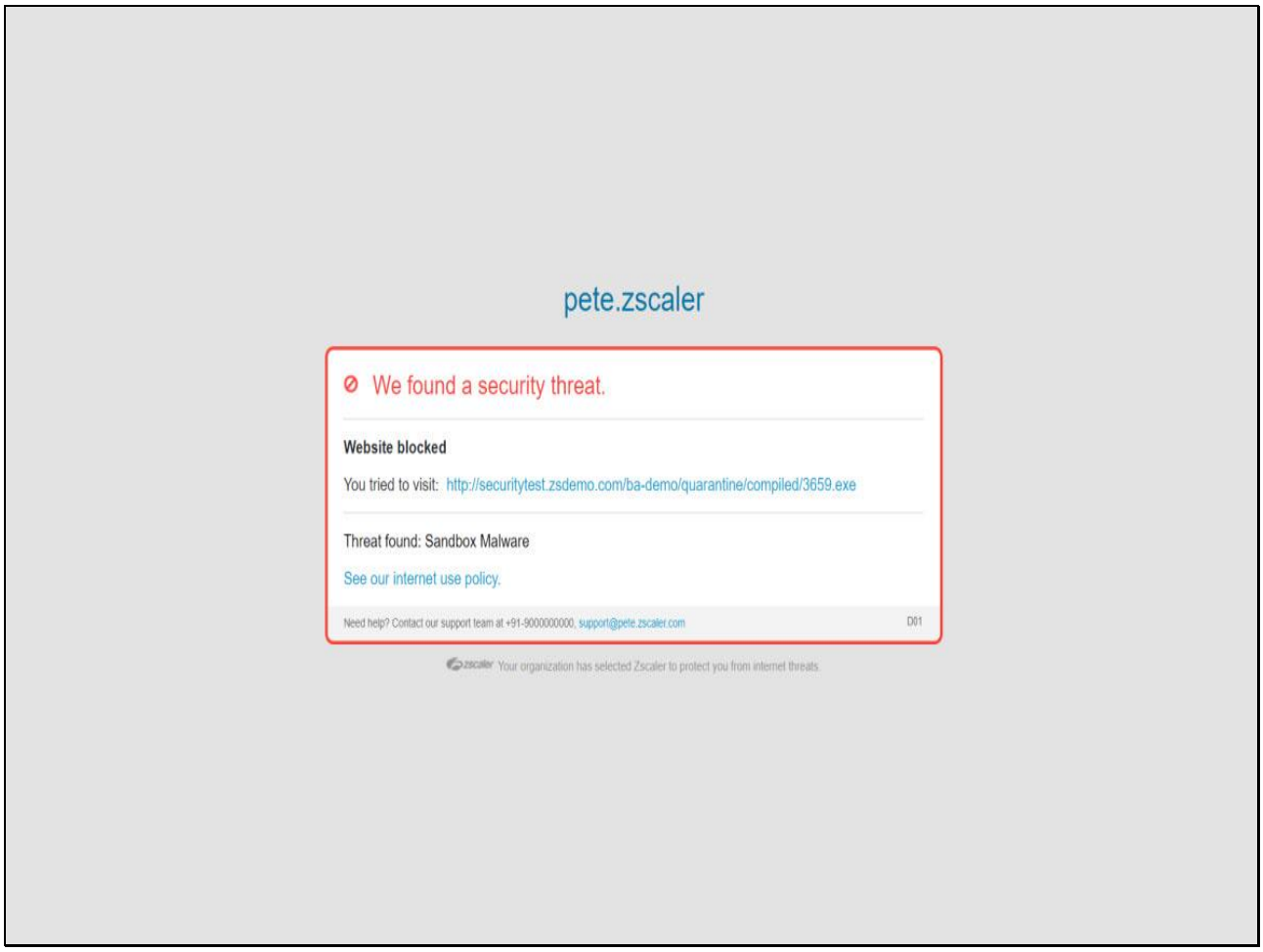
Slide 75 - Slide 75



Slide notes

For the end user experience, when the ‘Quarantine’ action is selected, they will see and ‘End User Notification’ (EUN) message while the file is being detonated. This page will refresh at intervals, …

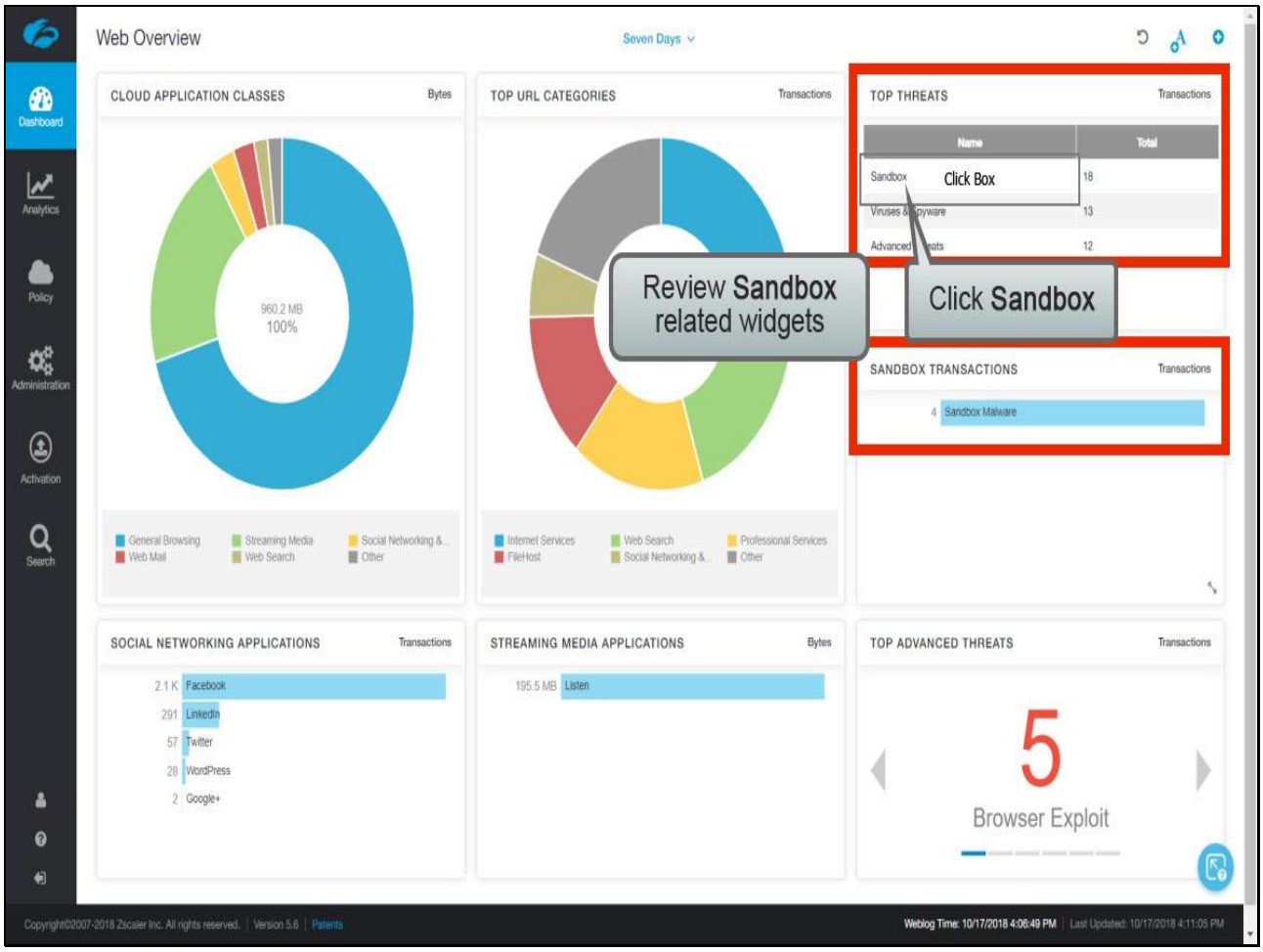
Slide 76 - Slide 76



Slide notes

…and if the file is found to be malicious a 'Block' EUN will be shown. If the file is found to be OK, it will simply be delivered.

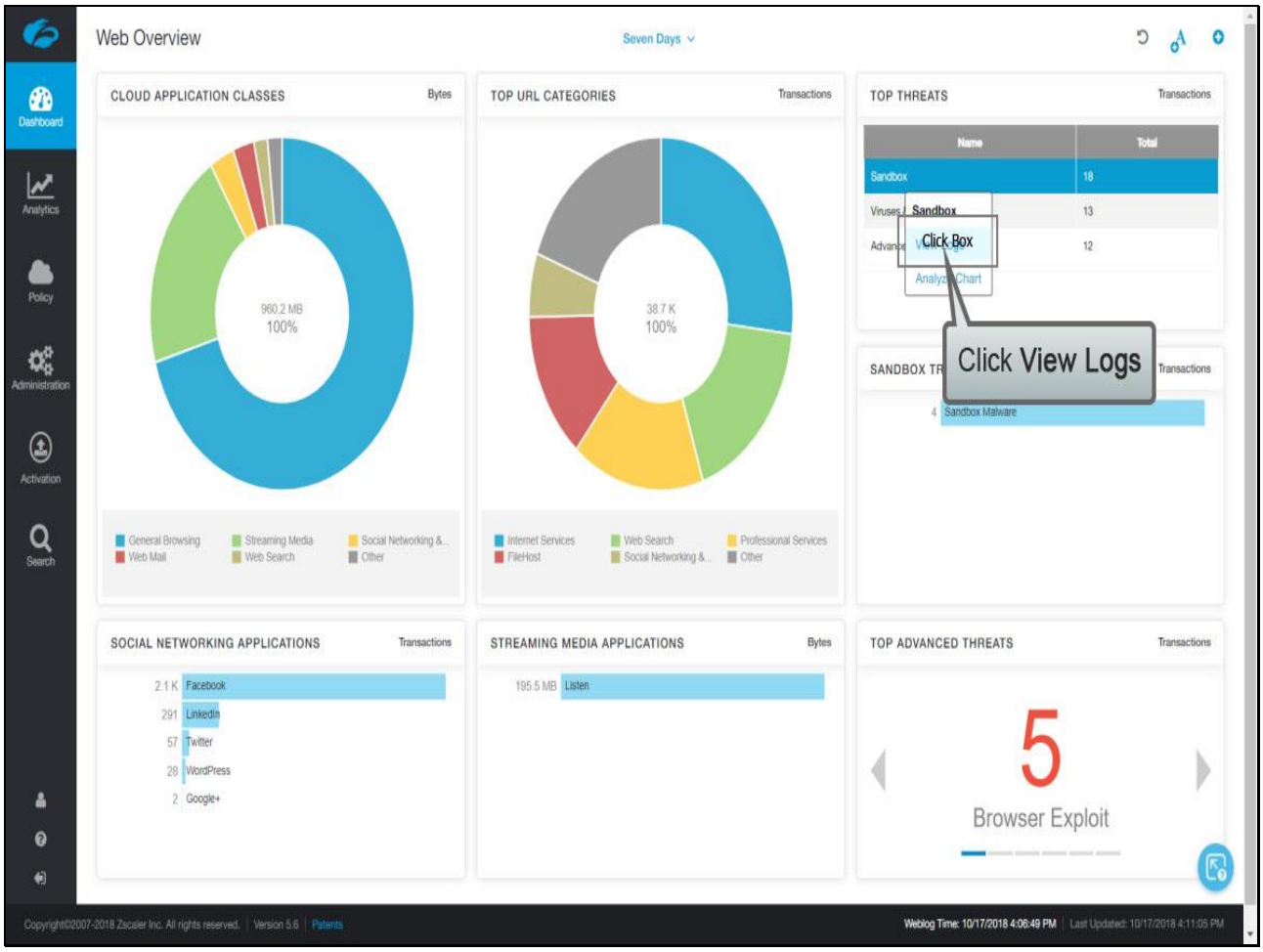
Slide 77 - Slide 77



Slide notes

An administrator with access to the Zscaler Admin Portal Dashboards, can review the Sandbox widgets on the ‘Web Overview’ Dashboard, and can drill down for full details. For example, in the 'Top Threats' widget, click ‘Sandbox’, …

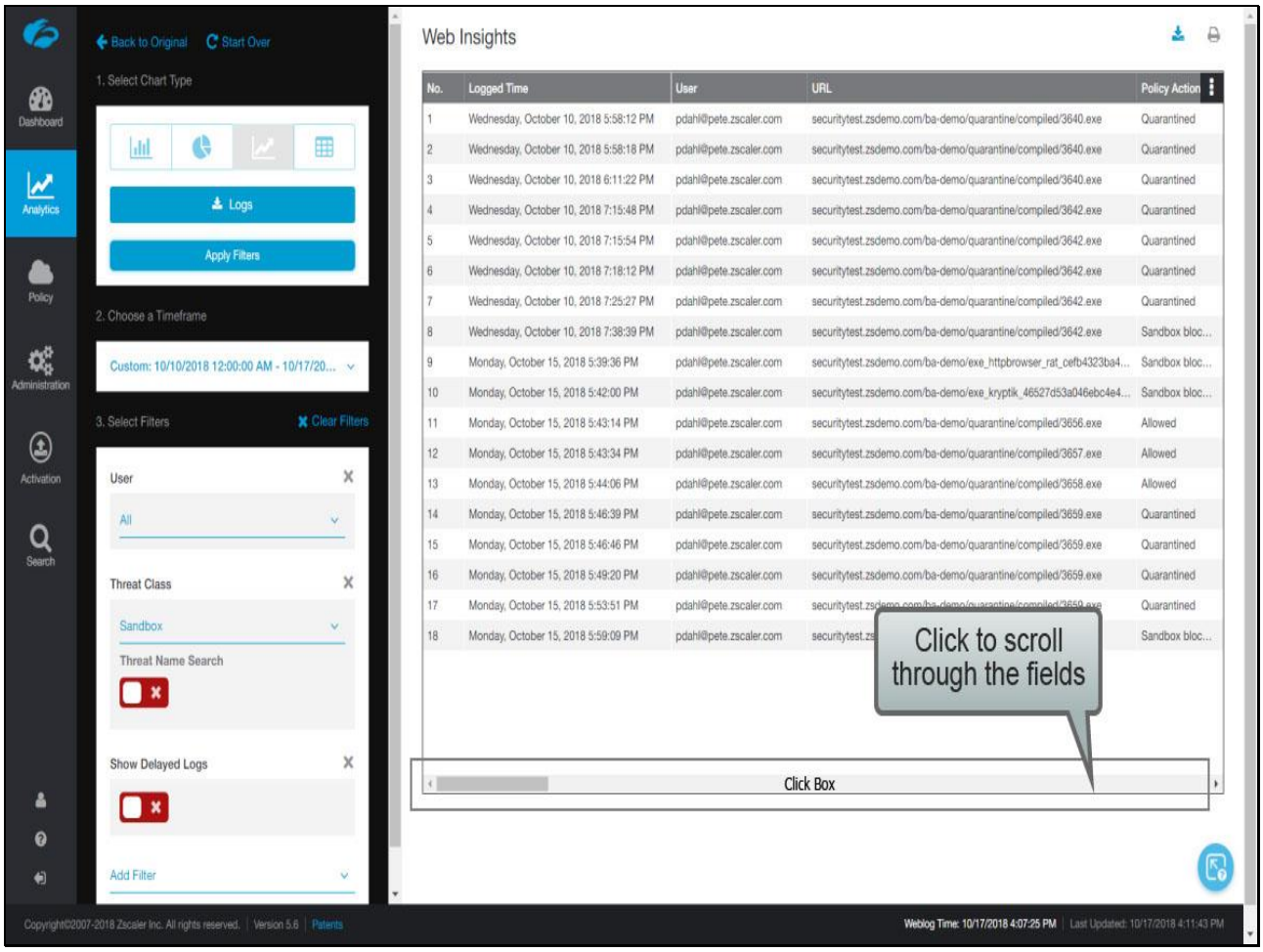
Slide 78 - Slide 78



Slide notes

…then click ‘View Logs’.

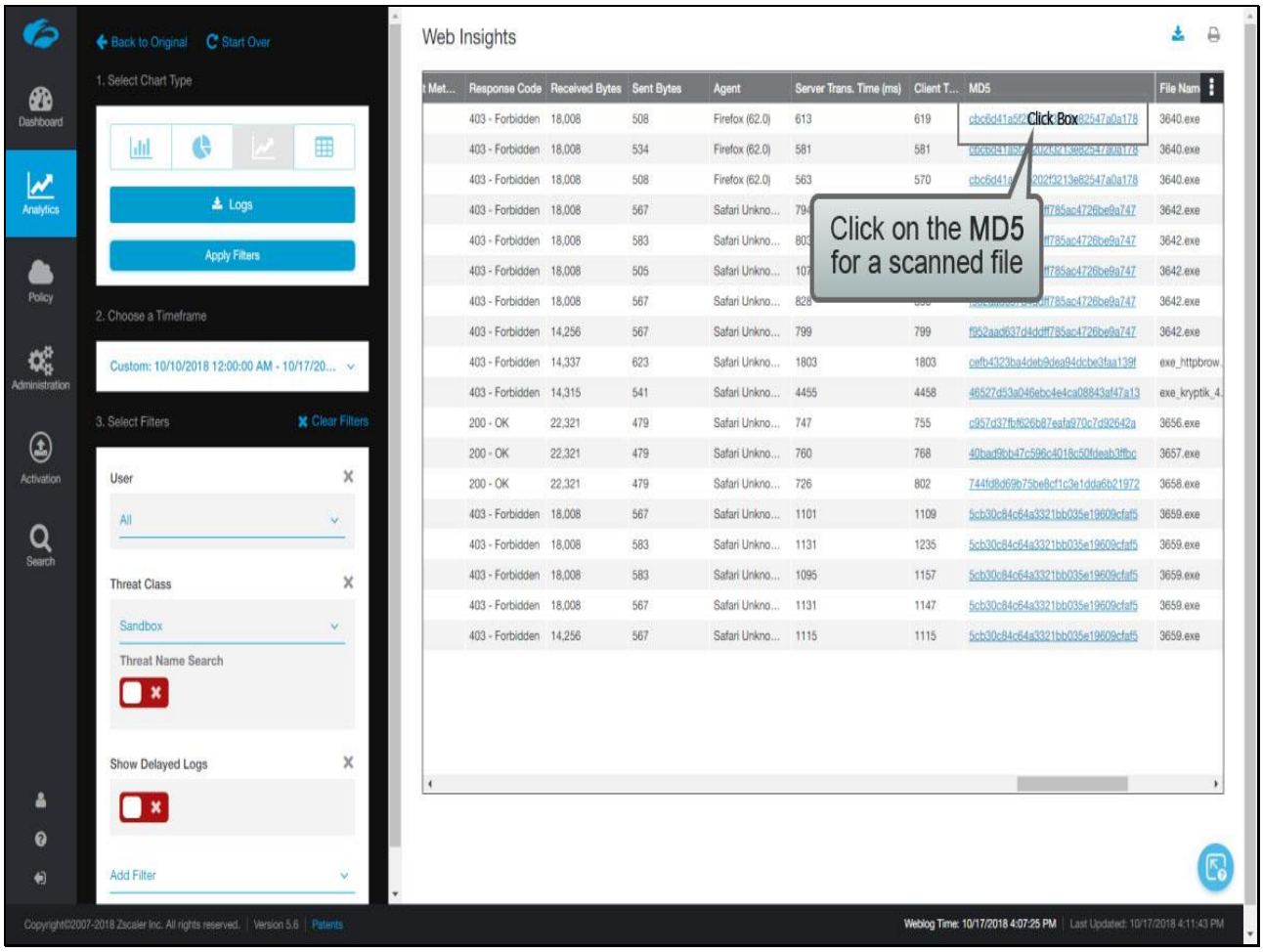
Slide 79 - Slide 79



Slide notes

Scroll through the data fields for the file, …

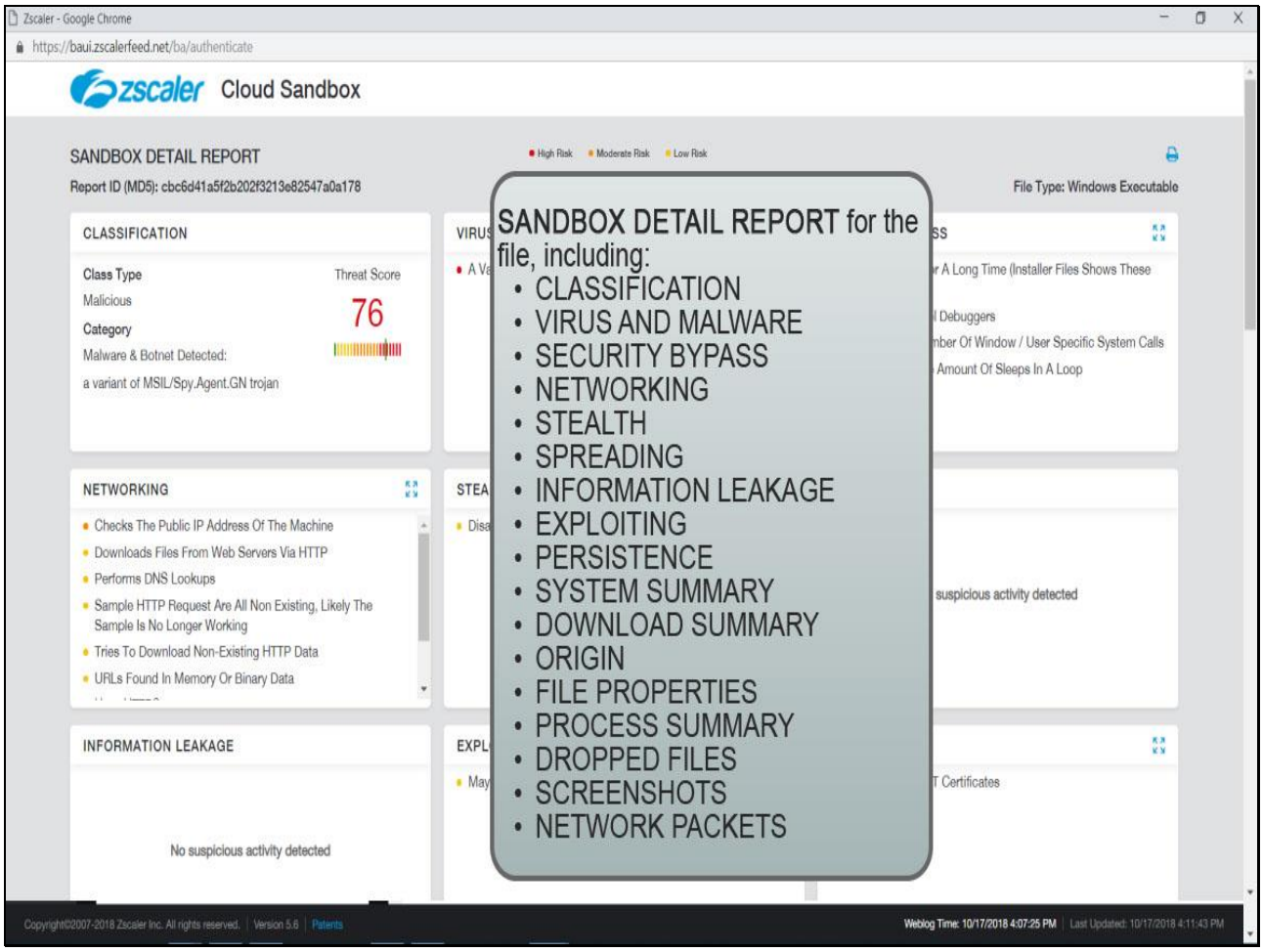
Slide 80 - Slide 80



Slide notes

…to find the ‘MD5’ field. To see a detailed Sandbox report on a file, click the link for its MD5 hash.

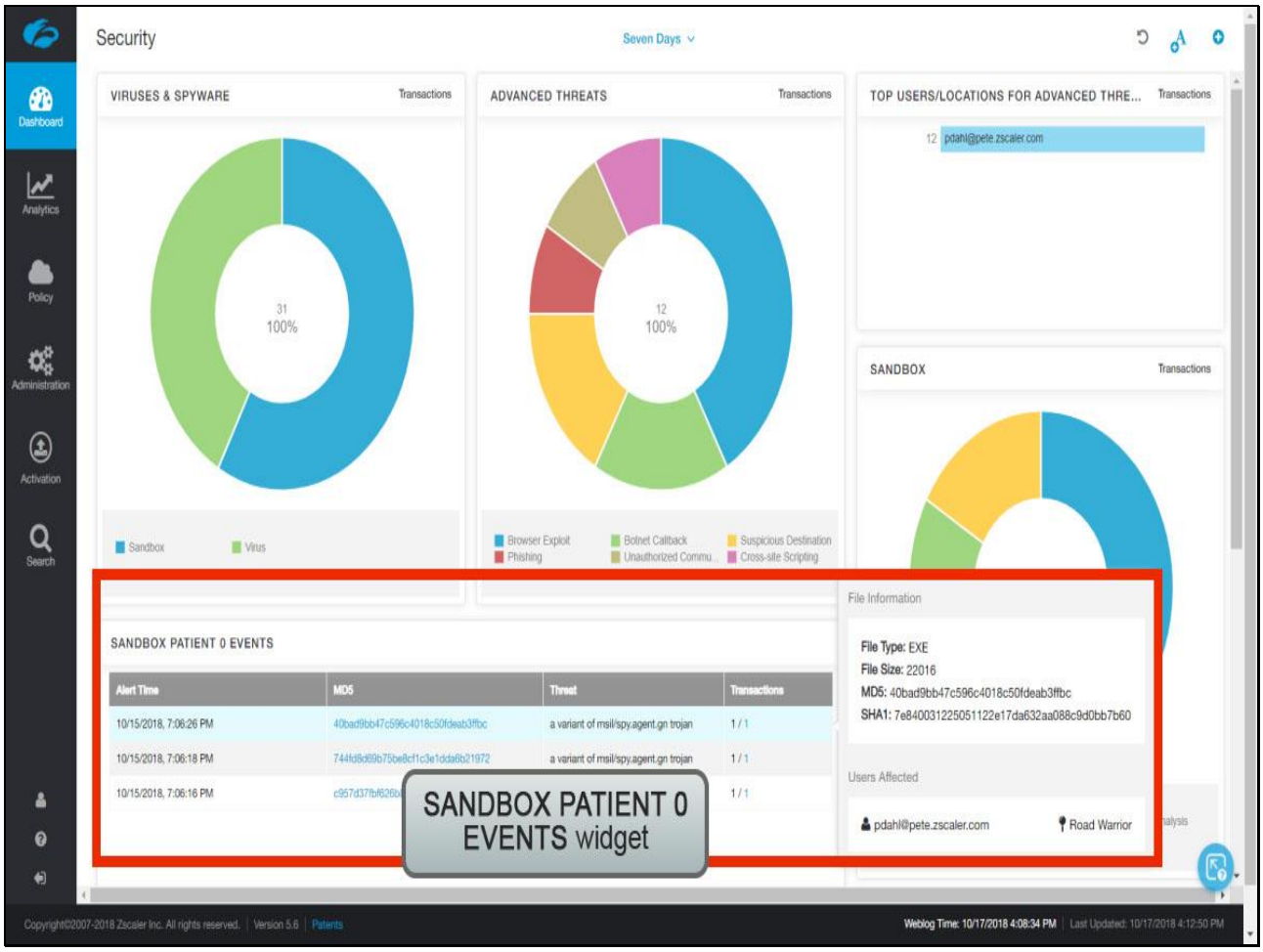
Slide 81 - Slide 81



Slide notes

The Sandbox details report for a file has full details on the behaviors observed when the file was detonated, including sections on: ‘CLASSIFICATION’, ‘VIRUS AND MALWARE’, ‘SECURITY BYPASS’, ‘NETWORKING’, ‘STEALTH’, ‘SPREADING’, ‘INFORMATION LEAKAGE’, ‘EXPLOITING', ‘PERSISTENCE’, ‘SYSTEM SUMMARY’, ‘DOWNLOAD SUMMARY’, ‘ORIGIN’, ‘FILE PROPERTIES’, ‘PROCESS SUMMARY’, ‘DROPPED FILES’, ‘SCREENSHOTS’, and ‘NETWORK PACKETS’.

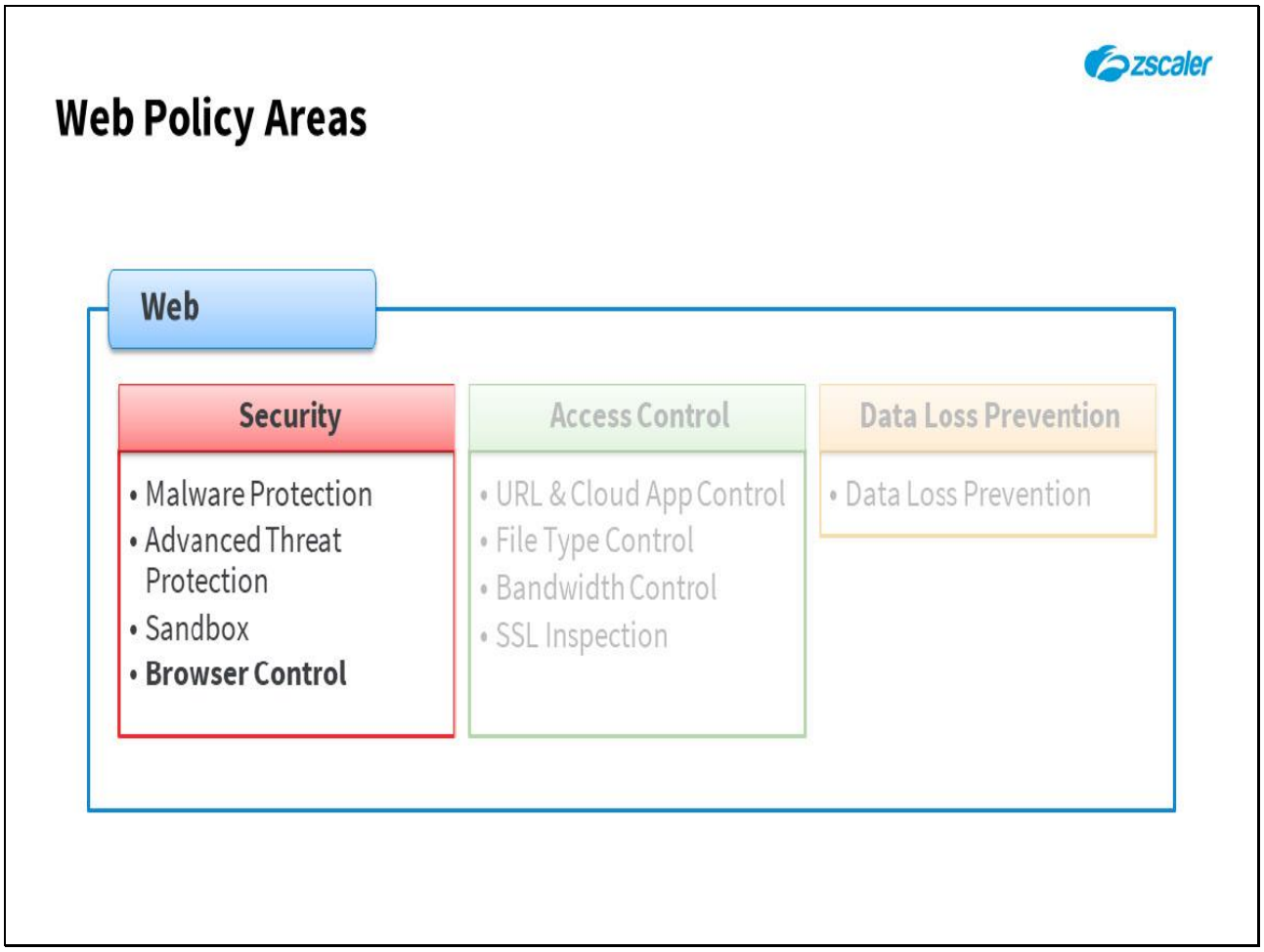
Slide 82 - Slide 82



Slide notes

In addition, the ‘Security’ Dashboard now has a ‘SANDBOX PATIENT 0 EVENTS’ widget, that provides full details for any ‘0 Day’ threats discovered by the Zscaler Cloud Sandbox.

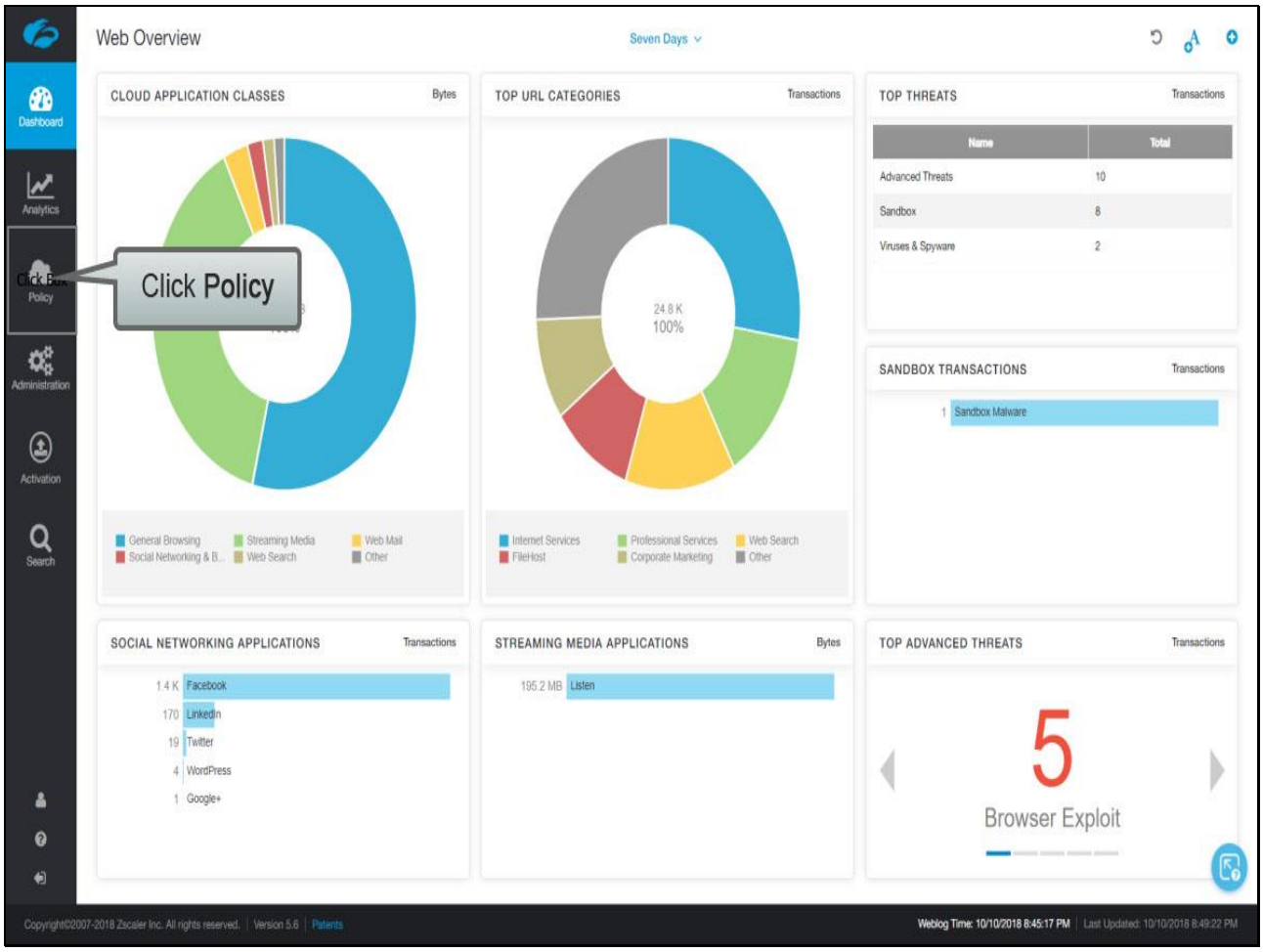
Slide 83 - Web Policy Areas



Slide notes

The 'Browser Control' Policy can be used to block older Browsers with known vulnerabilities that increase the security risk for your organization.

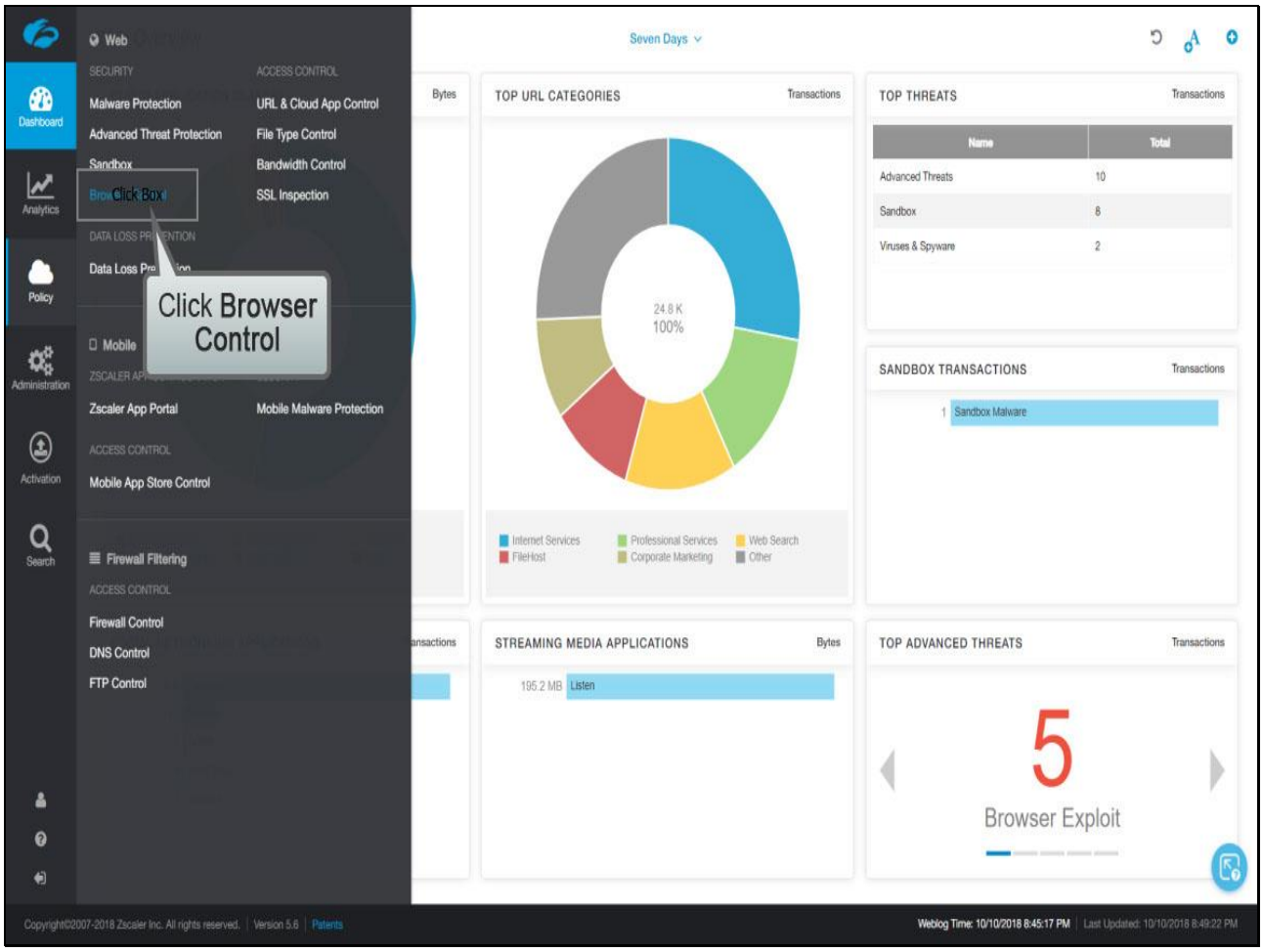
Slide 84 - Slide 84



Slide notes

To access the 'Browser Control' policy settings, click 'Policy', …

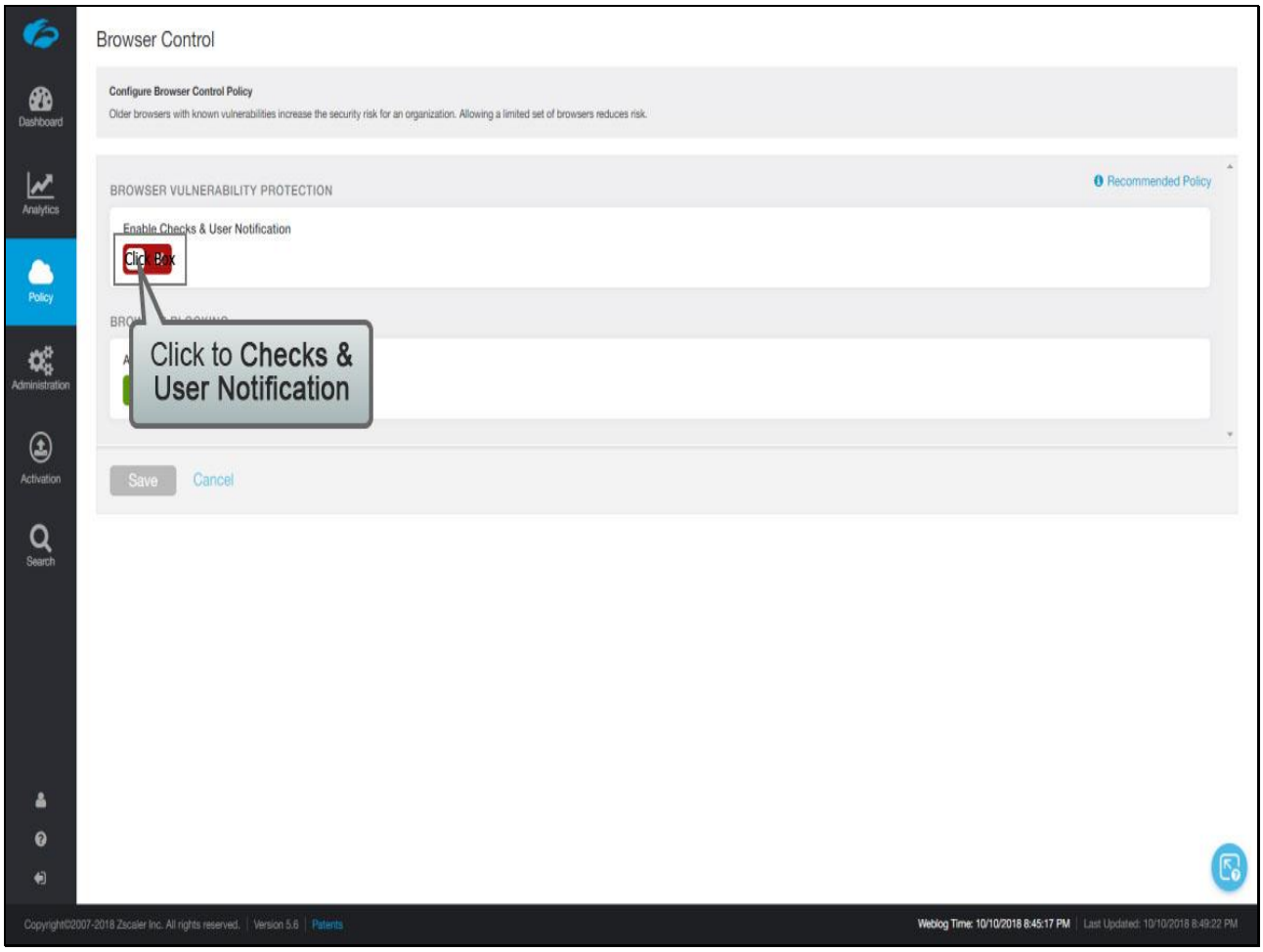
Slide 85 - Slide 85



Slide notes

…then from the ‘Web’ section of the ‘Policy’ menu, under the ‘SECURITY’ heading, click ‘Browser Control’.

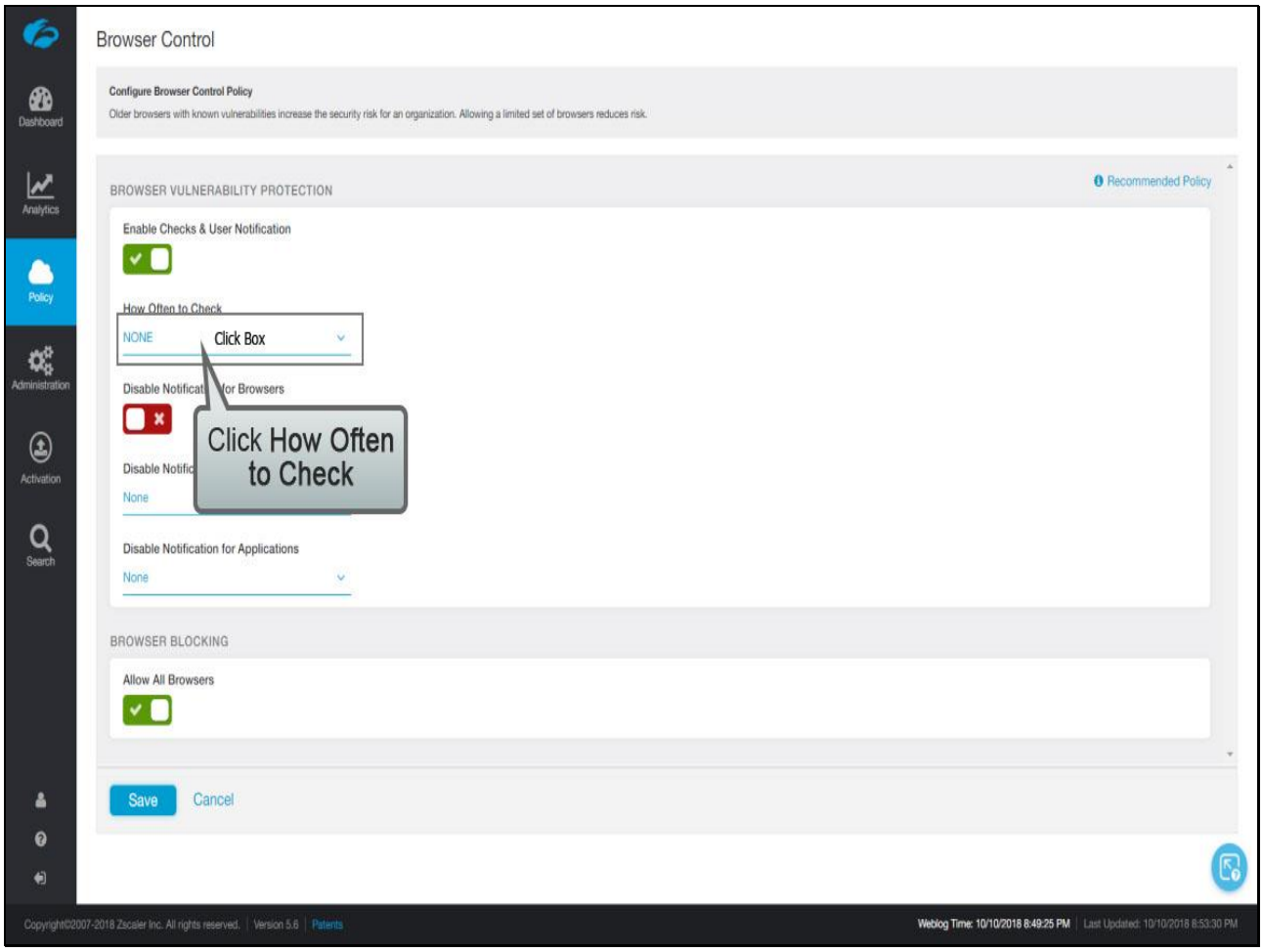
Slide 86 - Slide 86



Slide notes

To enable and configure browser 'Checks & User Notification', click to enable this option.

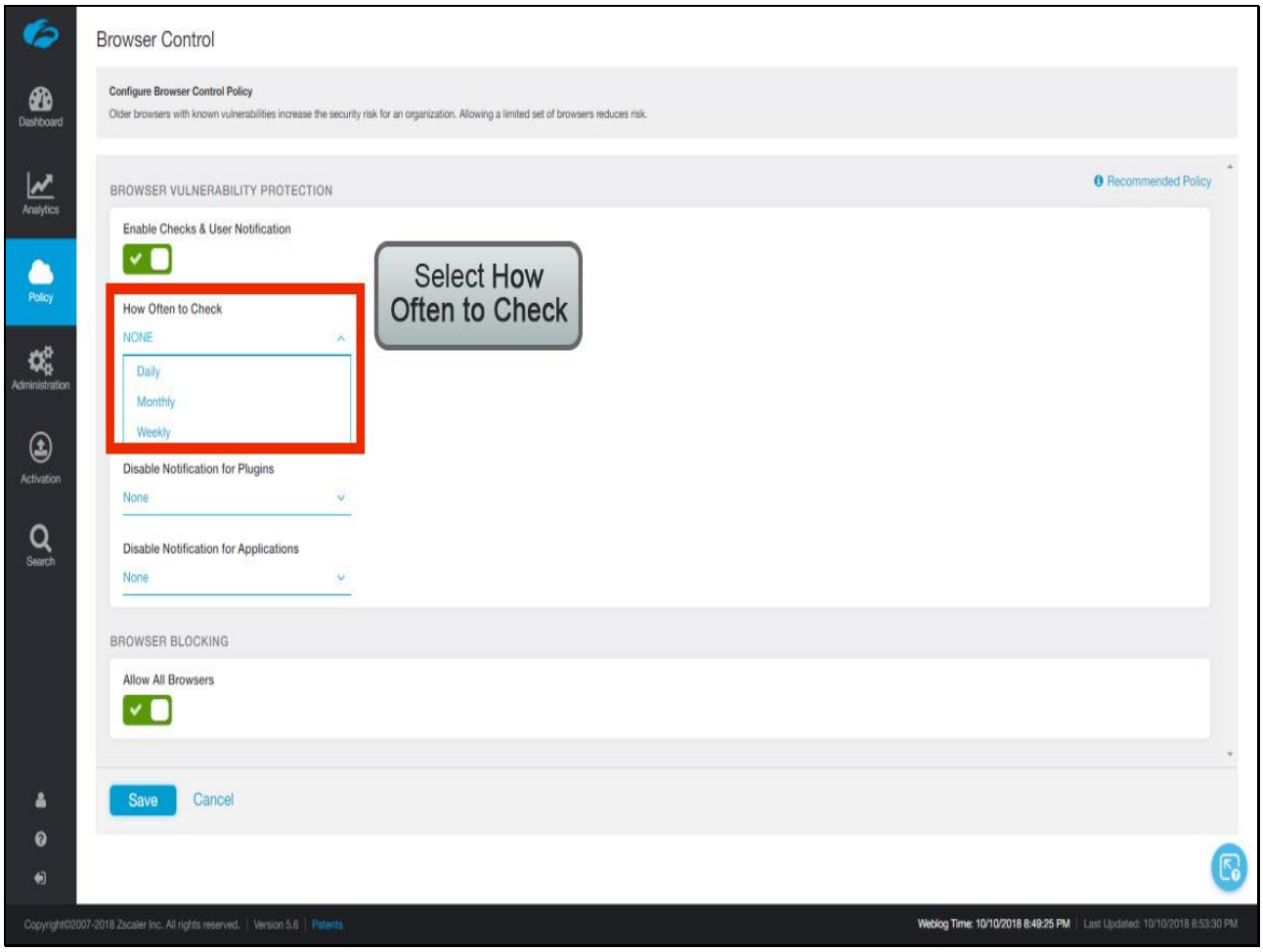
Slide 87 - Slide 87



Slide notes

To set a frequency to check end user browsers, click in the ‘How often to Check’ field, …

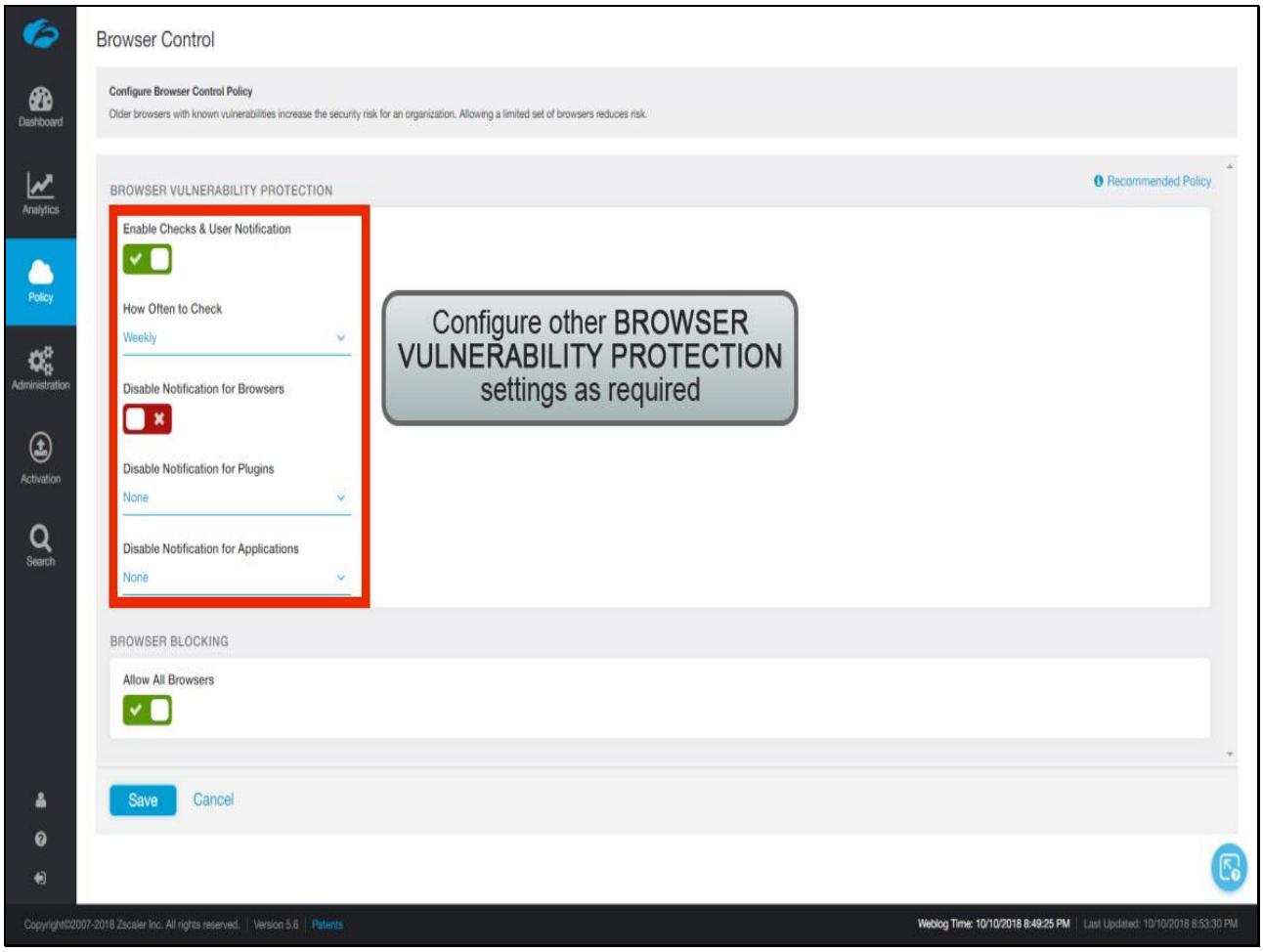
Slide 88 - Slide 88



Slide notes

…and select the required frequency (‘Daily’, ‘Monthly’ or ‘Weekly’).

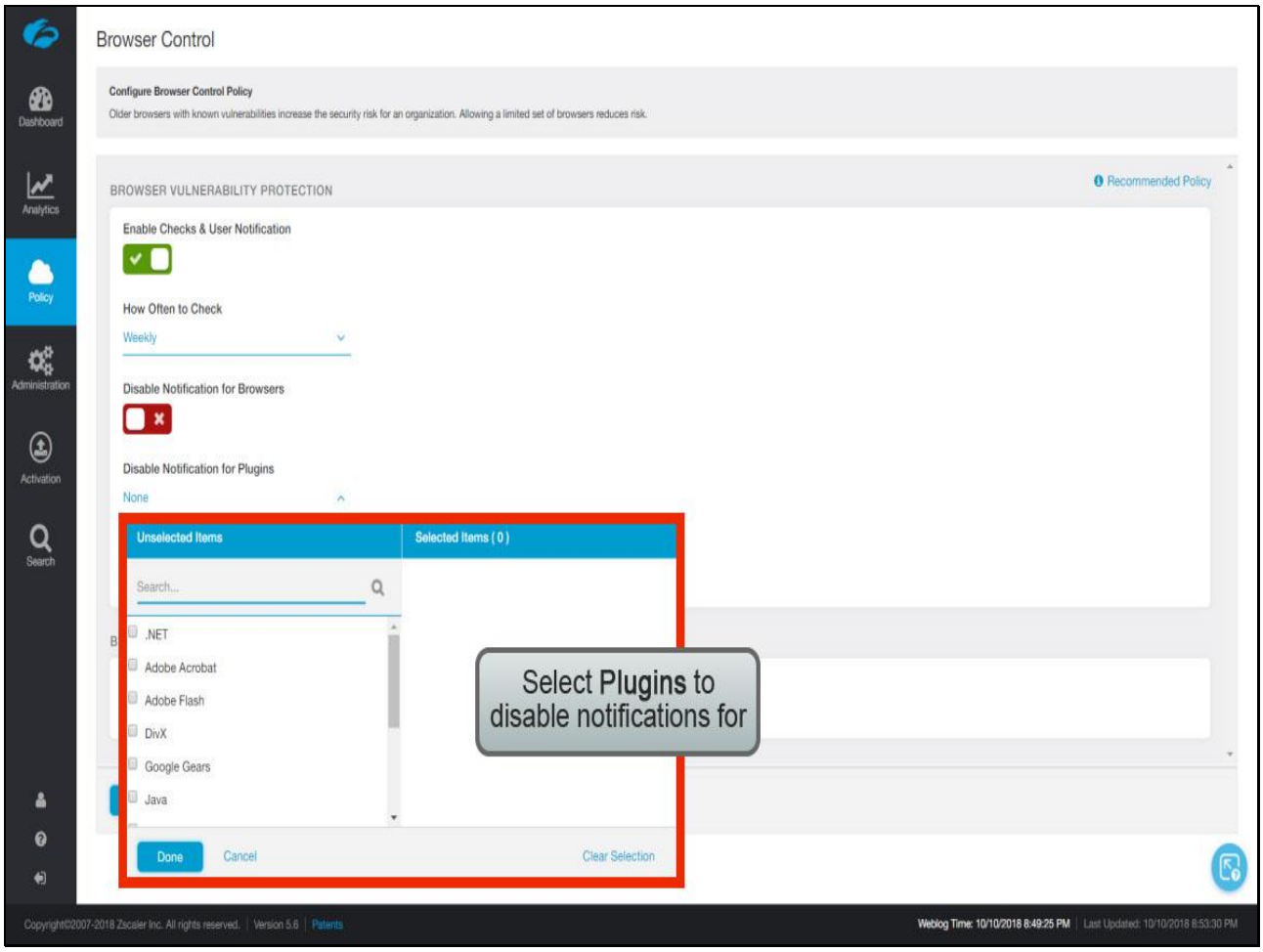
Slide 89 - Slide 89



Slide notes

Configure other 'BROWSER VULNERABILITY PROTECTION' settings as required, for example you can choose to 'Disable Notification for Browsers', …

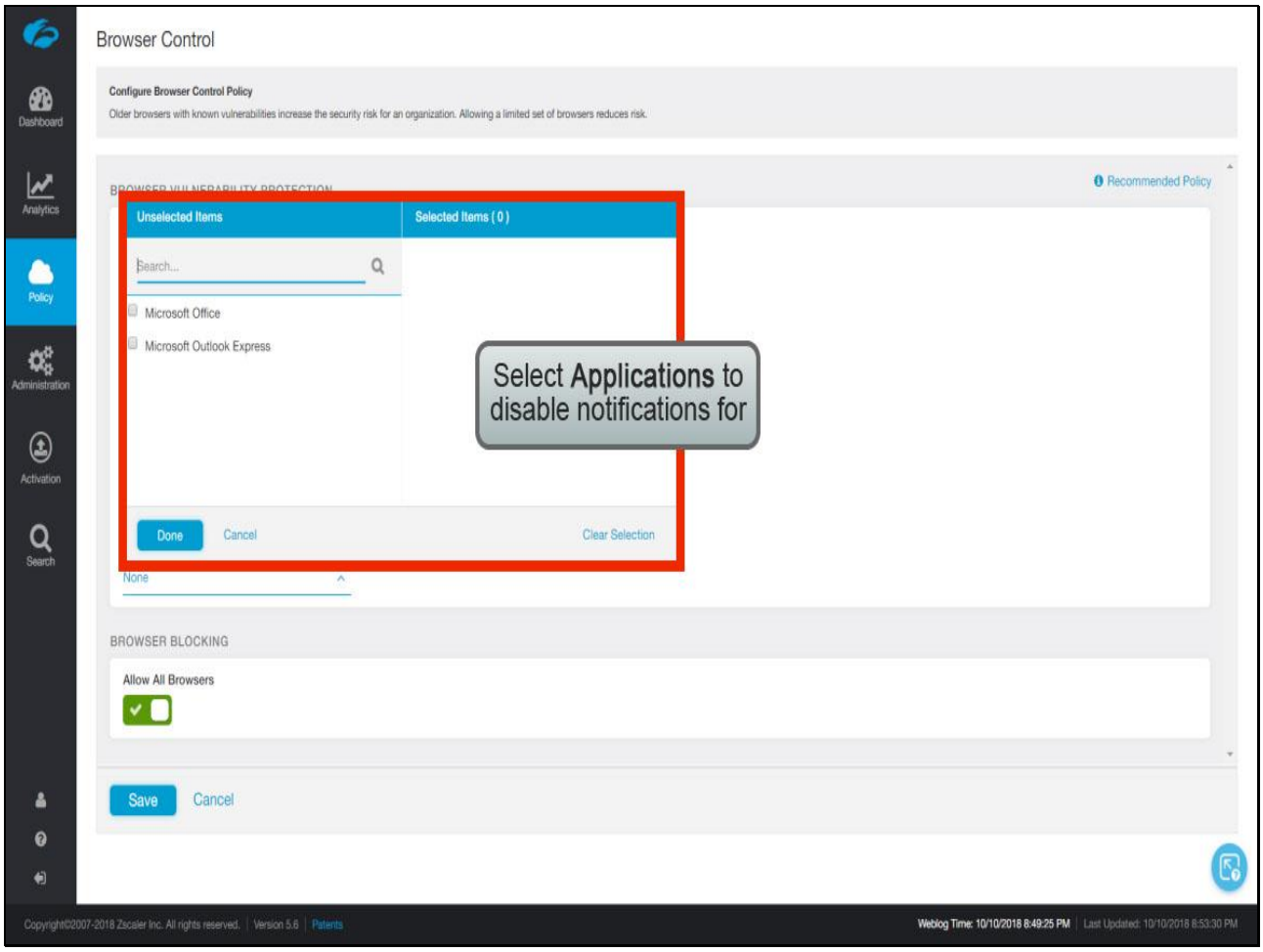
Slide 90 - Slide 90



Slide notes

…you can select individual plugins to disable notifications for, …

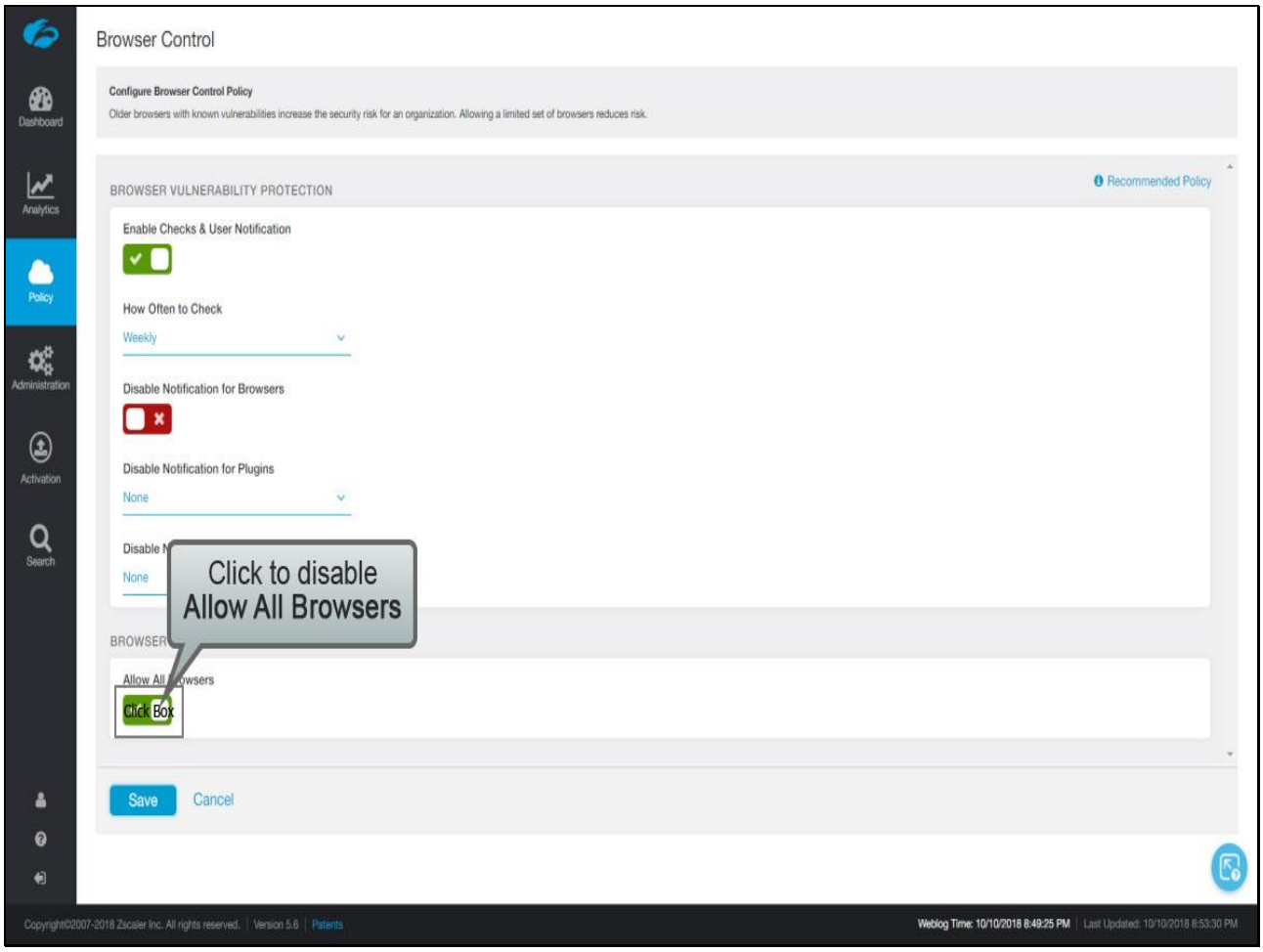
Slide 91 - Slide 91



Slide notes

…or you can select applications to disable notifications for.

Slide 92 - Slide 92

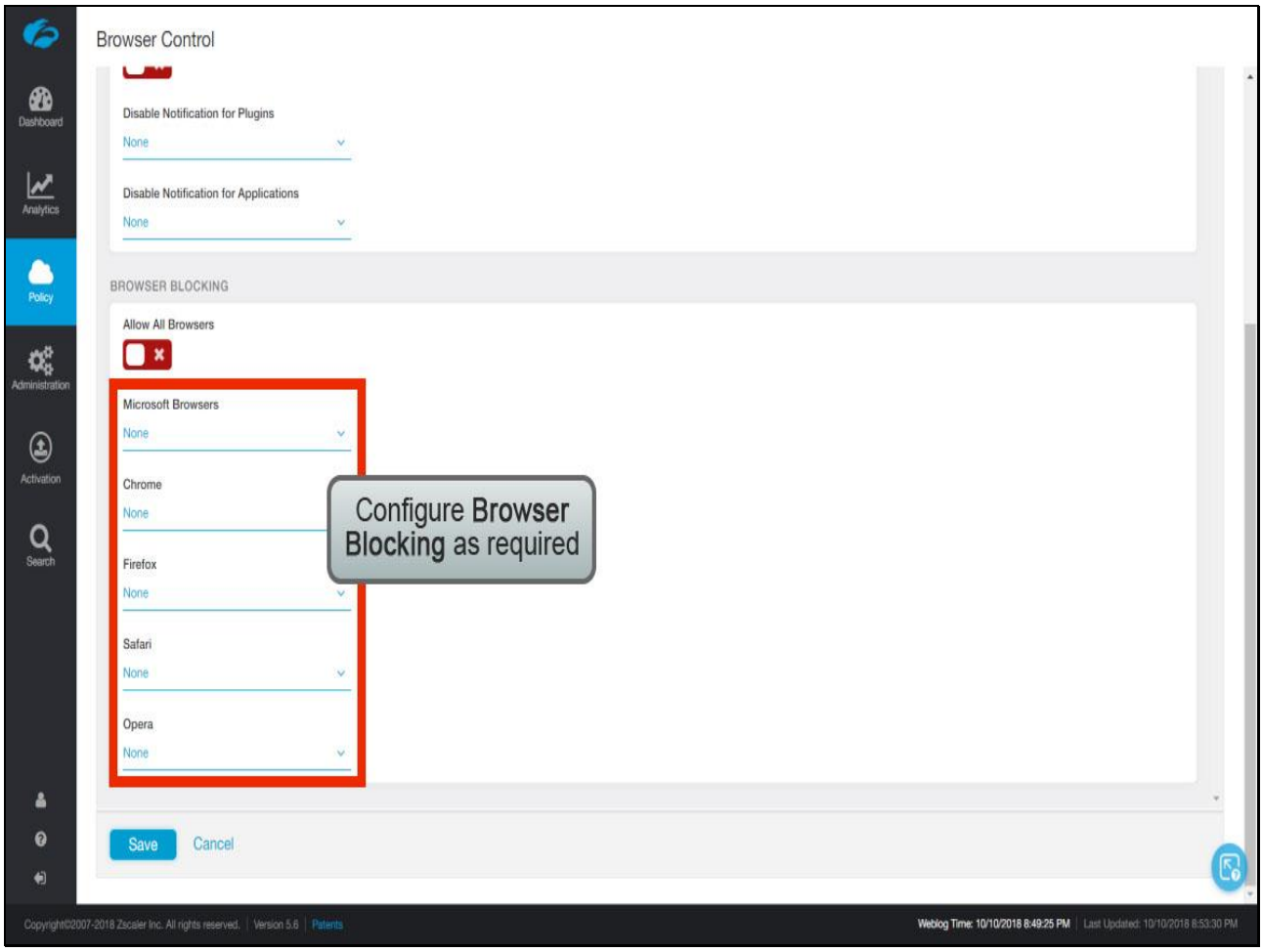


Slide notes

The next section allows you to specify which Browsers and Browser versions are permitted, although the default is to allow all Browsers. The Browsers available to select are: ‘Microsoft Browsers’ (IE and Edge); ‘Chrome’; ‘Firefox’; ‘Safari’; and ‘Opera’.

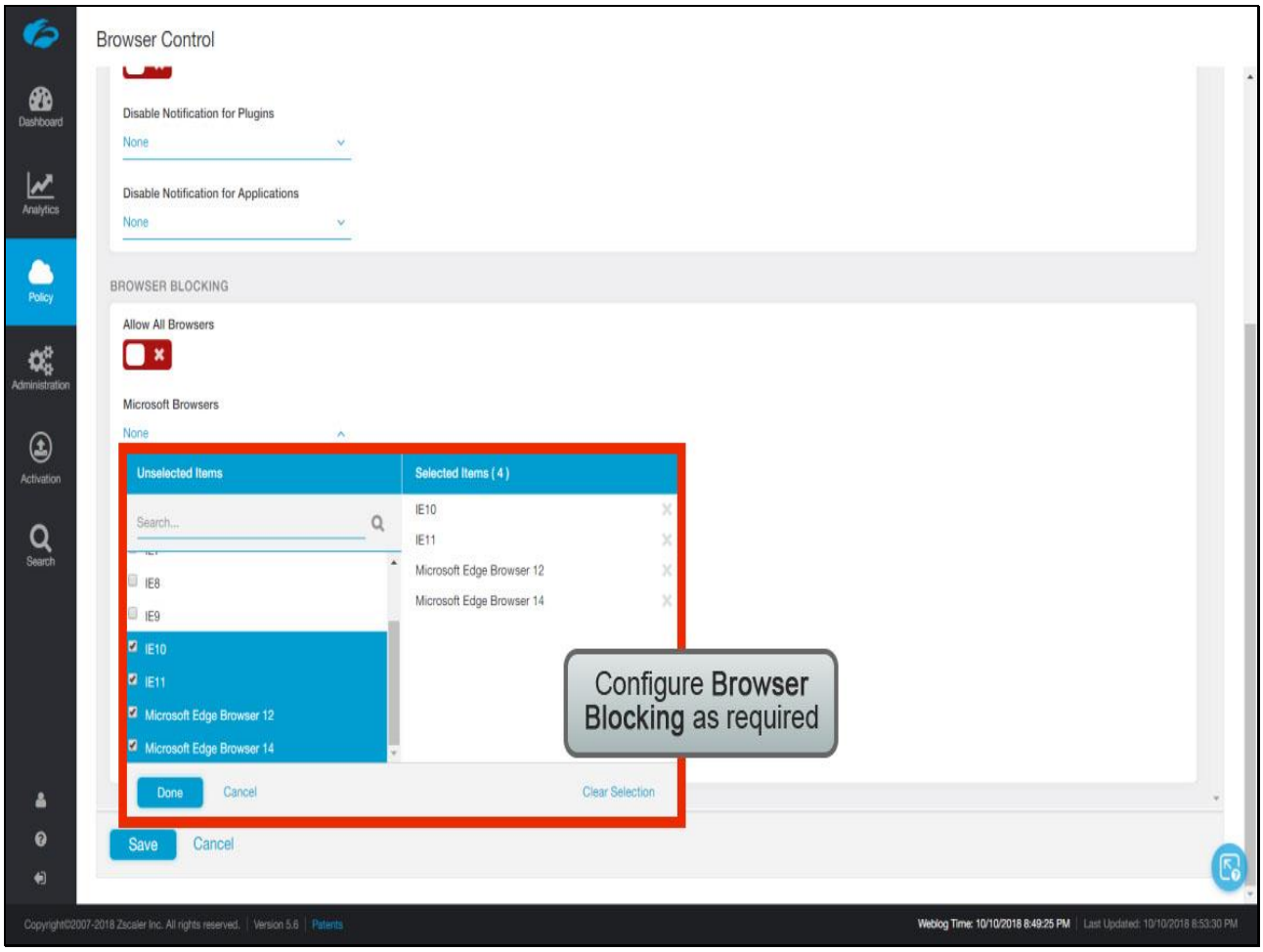
To configure browser restrictions, click to disable the ‘Allow All Browsers’ option, …

Slide 93 - Slide 93



Slide notes

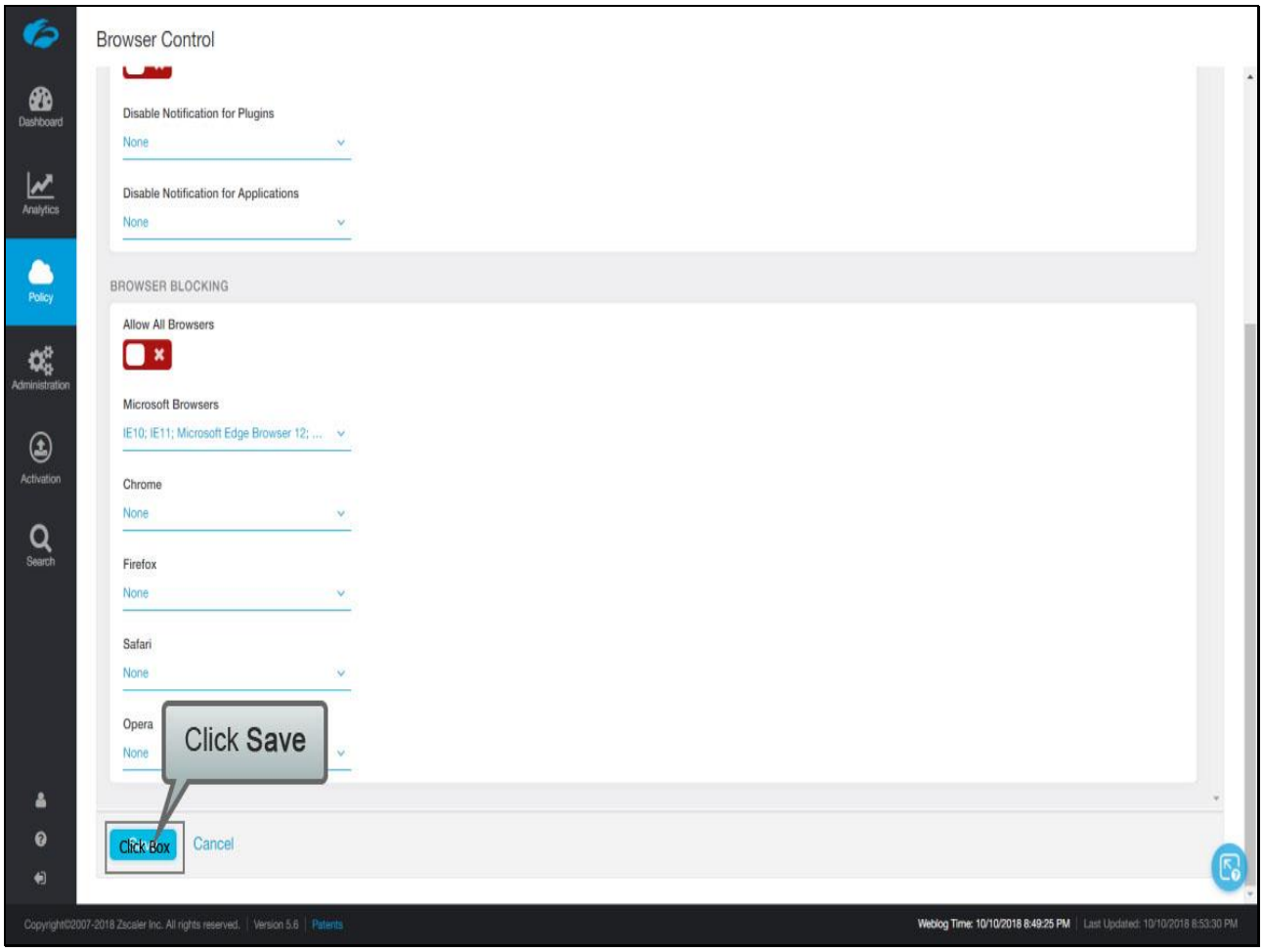
Slide 94 - Slide 94



Slide notes

…configure the Browser versions that you wish to block, ...

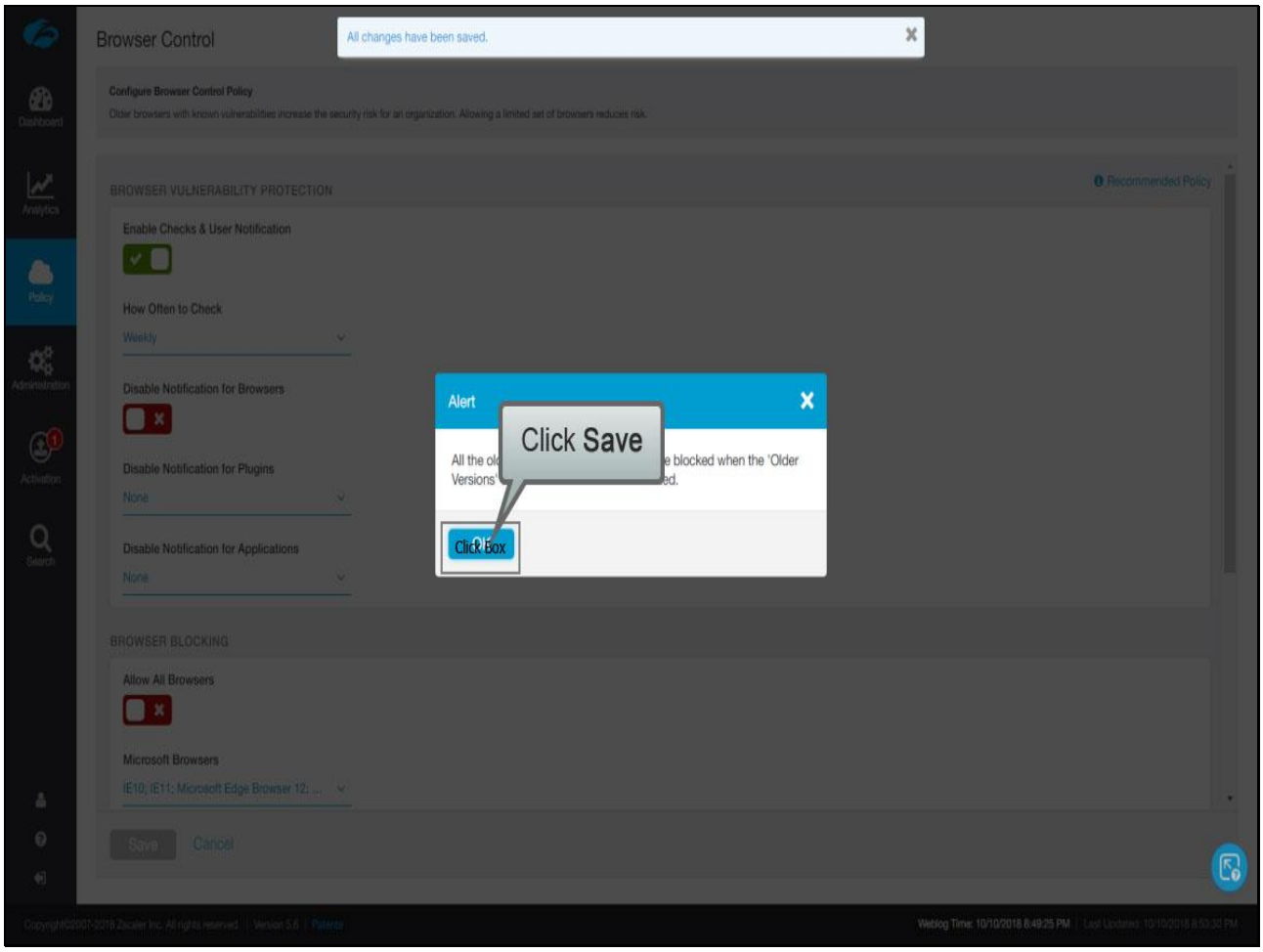
Slide 95 - Slide 95



Slide notes

…then 'Save' the configuration, …

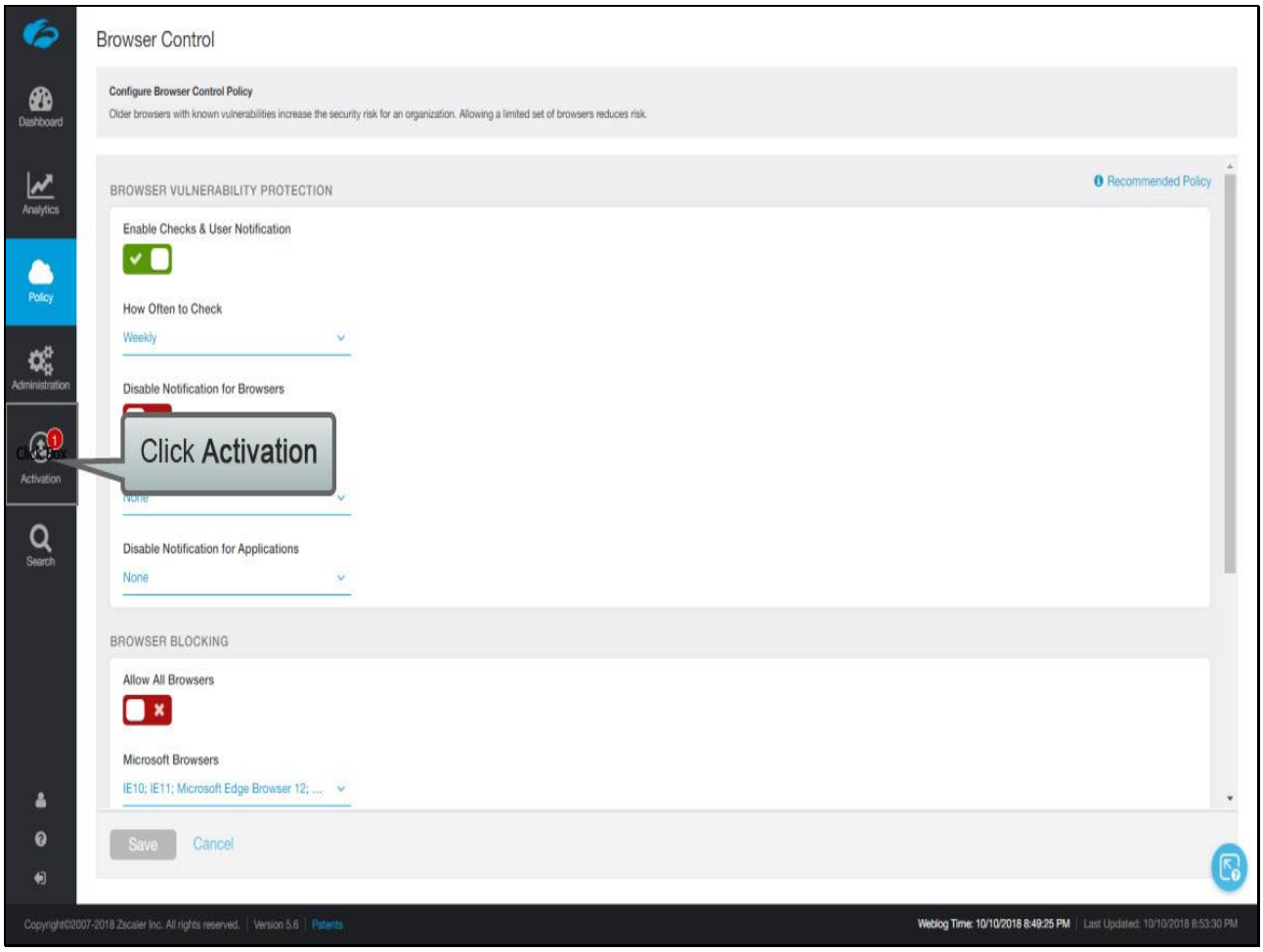
Slide 96 - Slide 96



Slide notes

...and click 'OK' to clear the warning message.

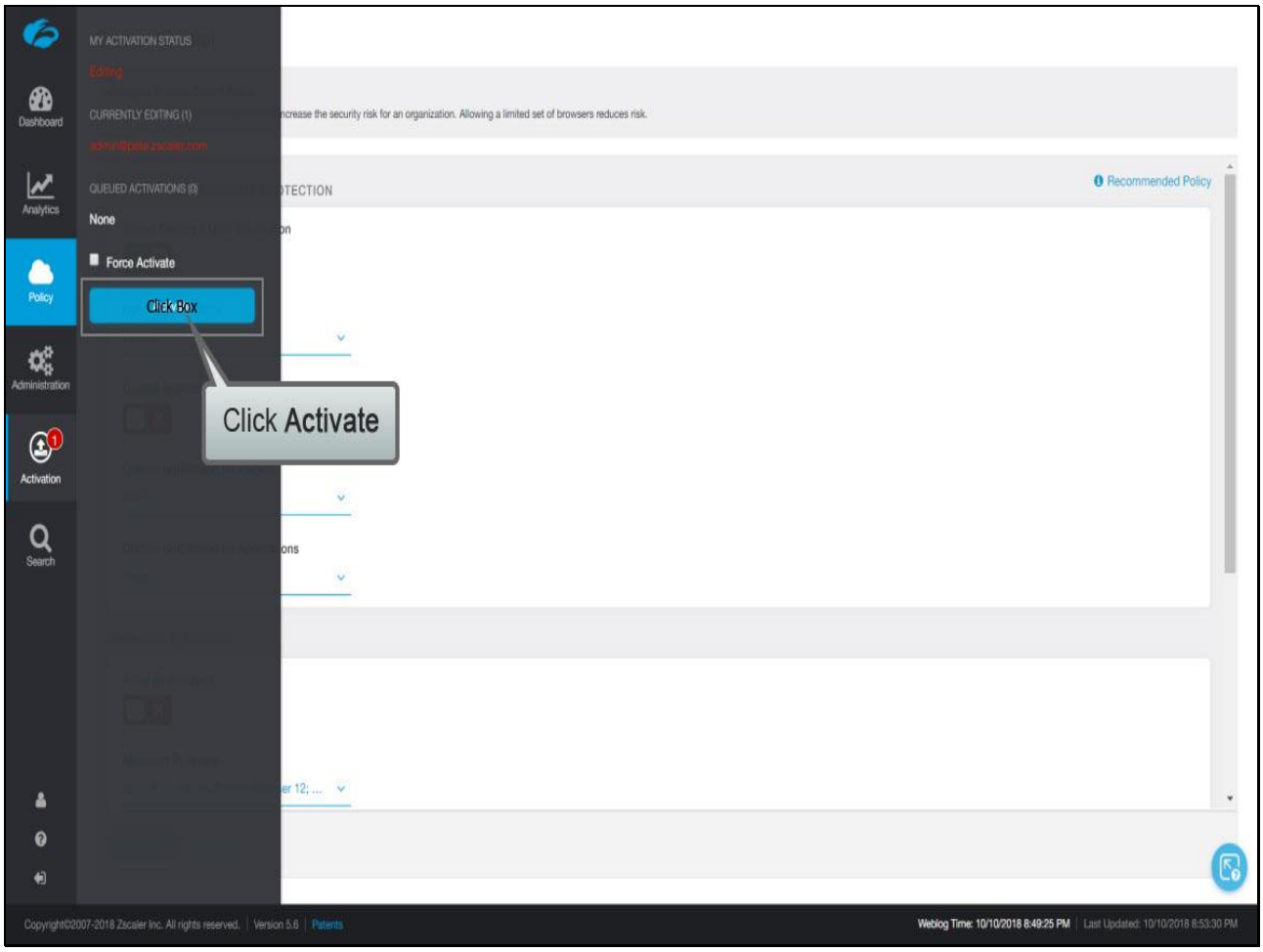
Slide 97 - Slide 97



Slide notes

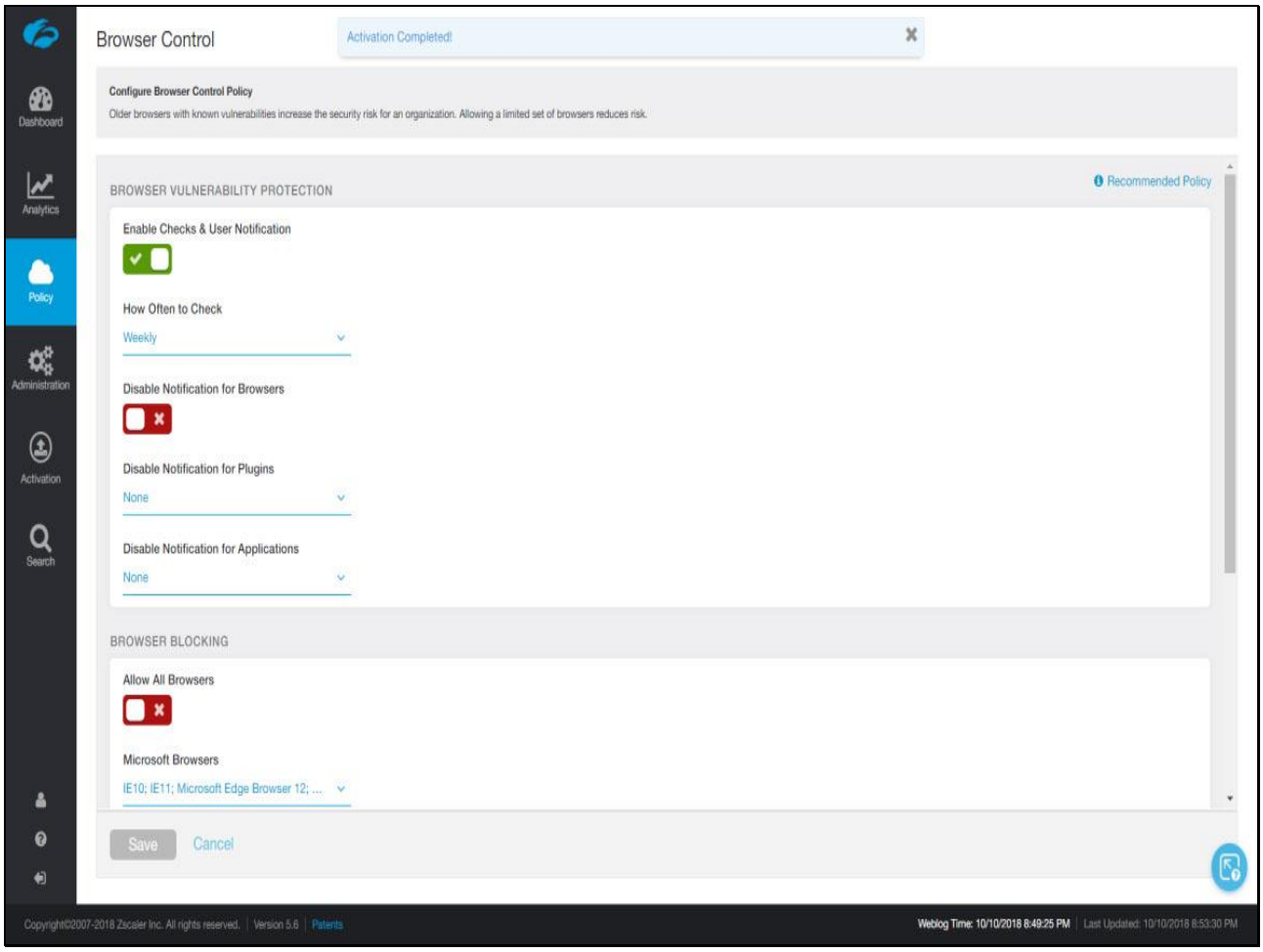
Then Activate your changes.

Slide 98 - Slide 98



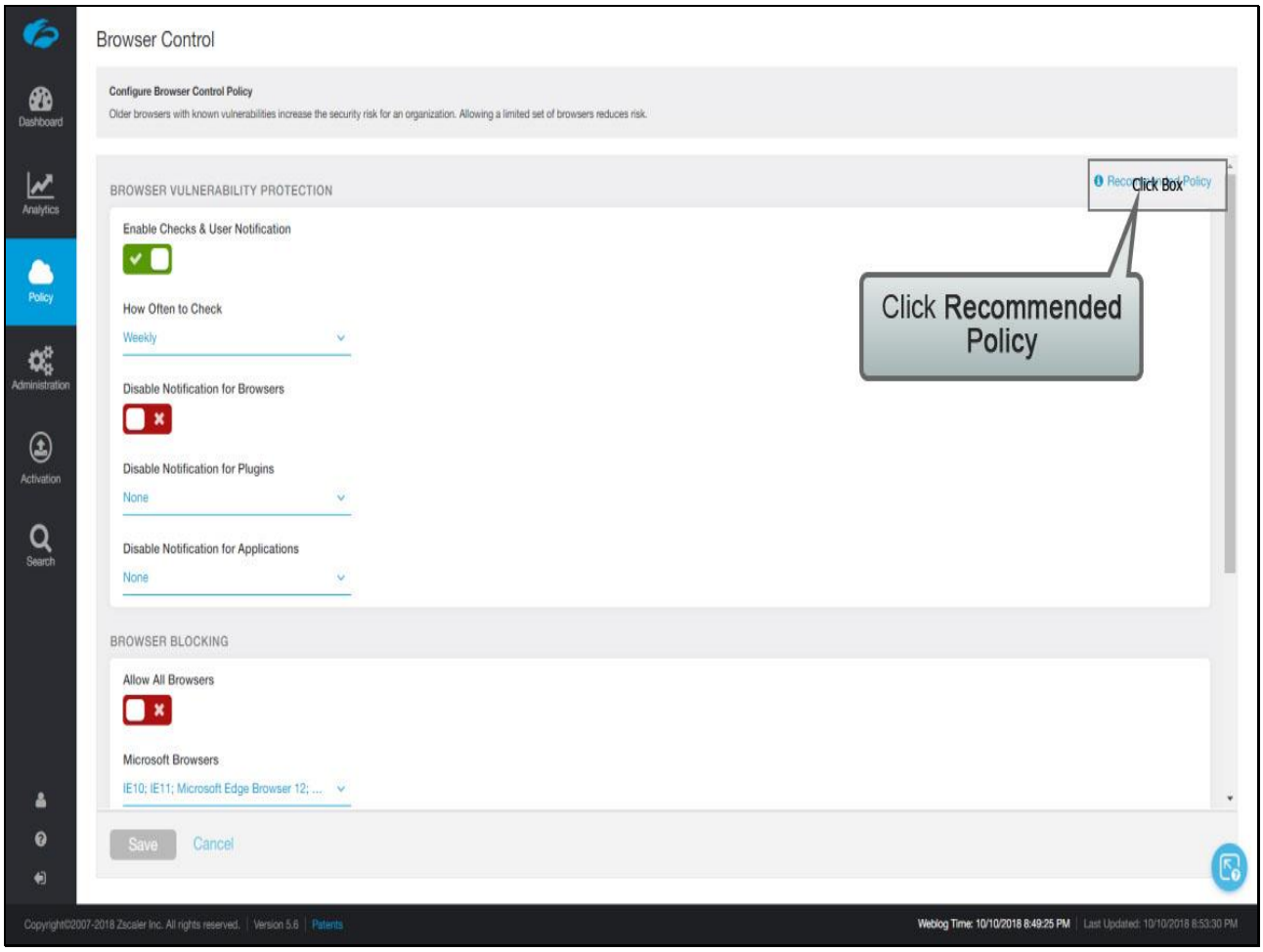
Slide notes

Slide 99 - Slide 99



Slide notes

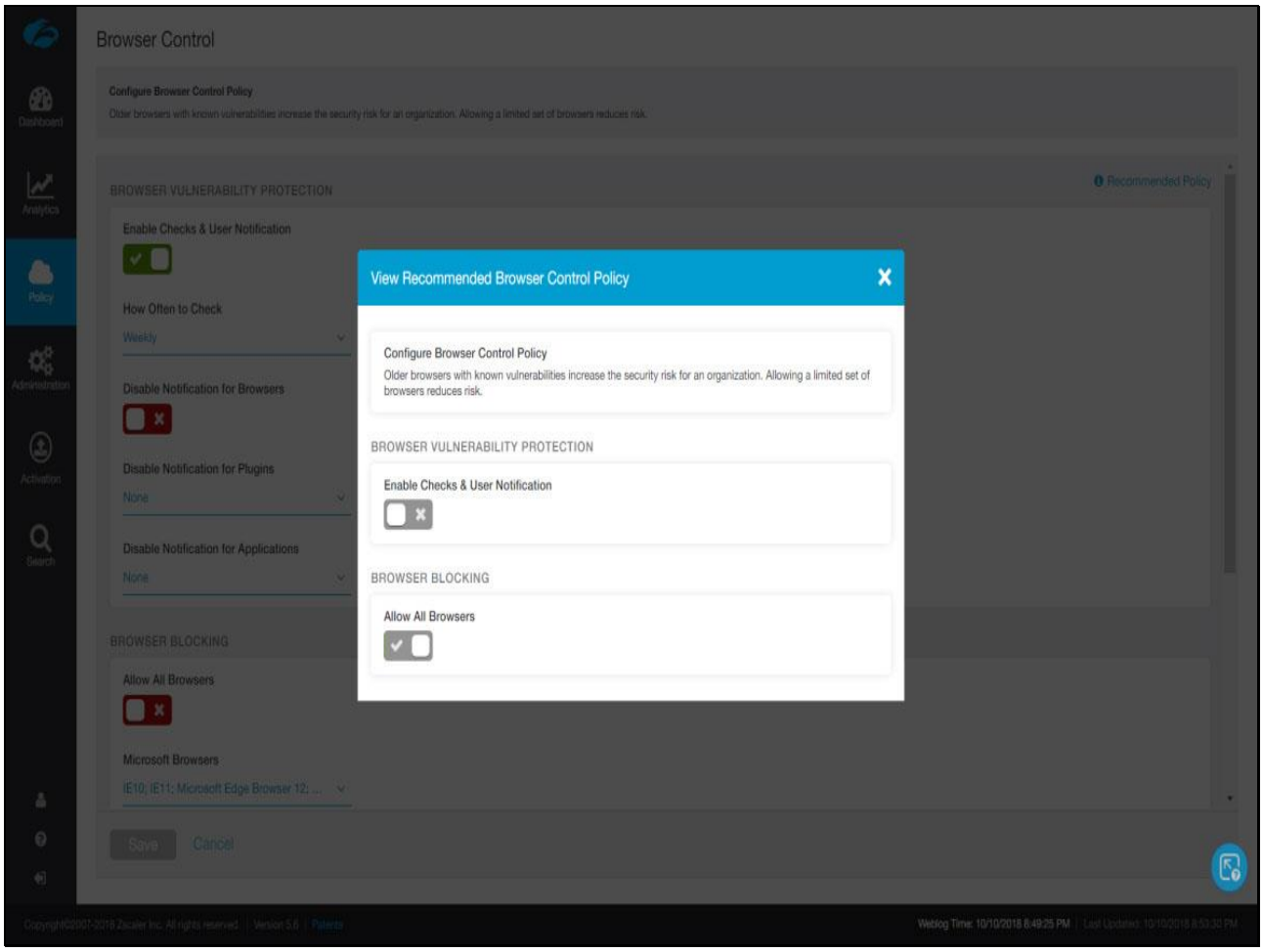
Slide 100 - Slide 100



Slide notes

To see Zscaler recommendations for configuring 'Browser Control' Policy settings, click the 'Recommended Policy' link.

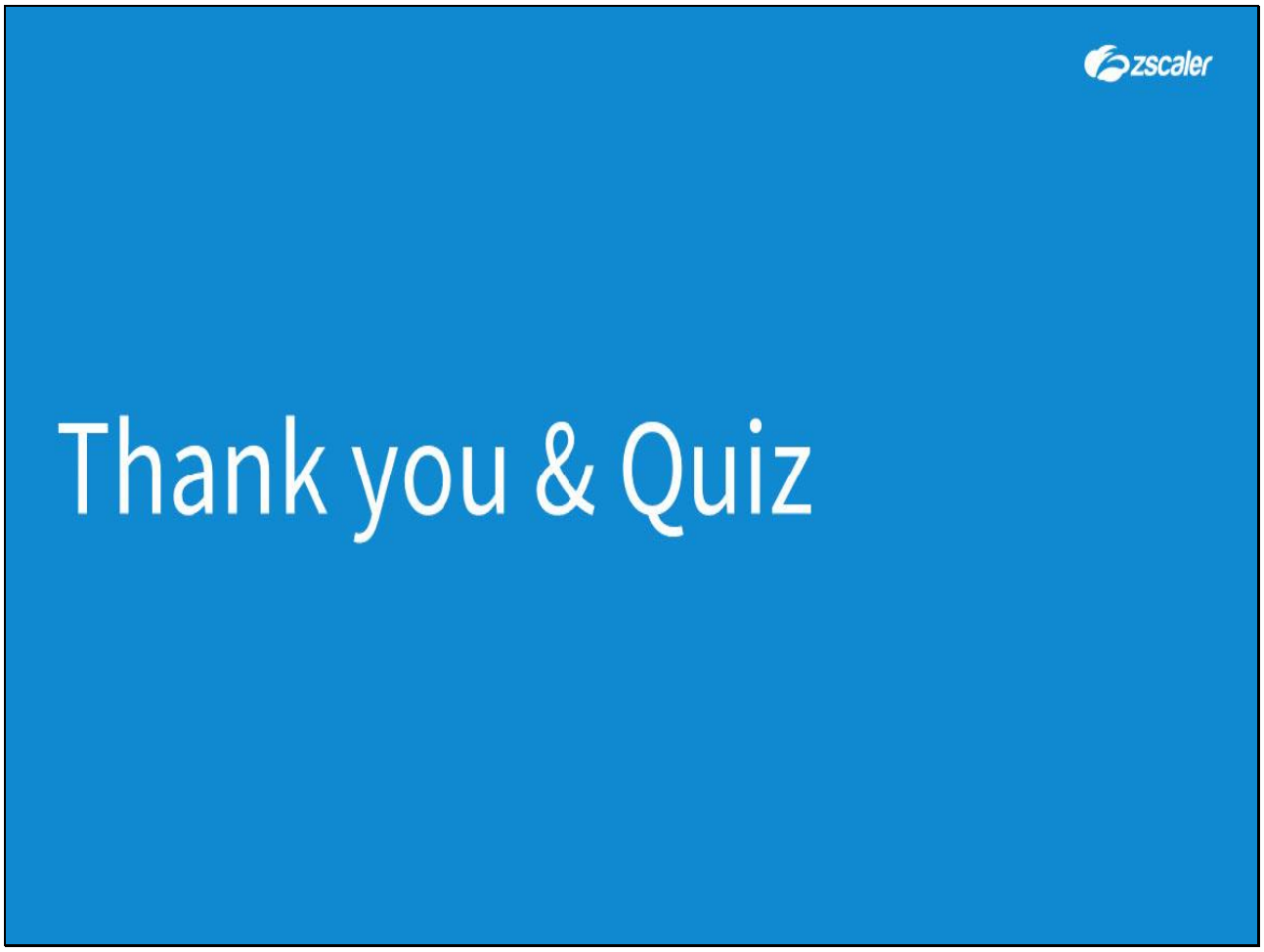
Slide 101 - Slide 101



Slide notes

For the 'Browser Control' Policy Zscaler recommends that you disable checks and user notification and allow all Browsers.

Slide 102 - Thank you & Quiz



Slide notes

Thank you for following this Zscaler training module, we hope this module has been useful to you and thank you for your time.

Click the 'X' at top right to close this interface, then launch the quiz to test your knowledge of the material presented during this module. You may retake the quiz as many times as necessary in order to pass.