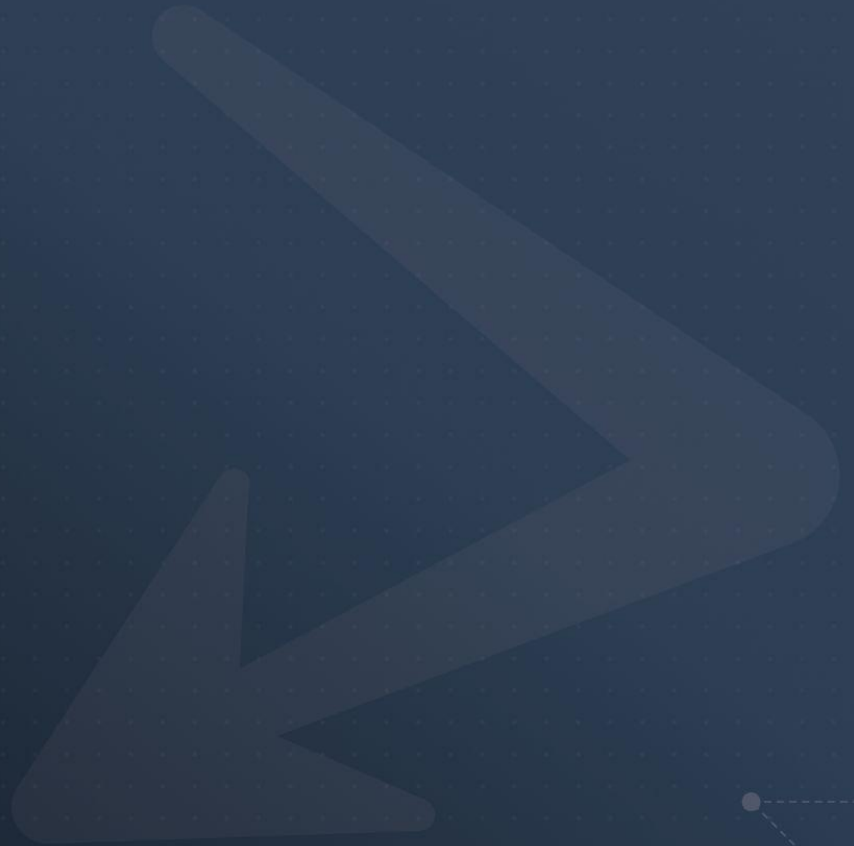# ThreatBlockr Redesign

Key Updates & New Features

February 2023

Key Updates to Existing Features:

Improved Policy Configuration

Policies will be easier to configure! Whether creating a new policy or making configuration updates to an existing one, the process has been simplified and each configuration step will be fully transparent.

Lists Consolidation

Allow, Block & Threat Lists will be consolidated into one left-hand navigation menu item. Each list type will be accessed by selecting the desired List type tab (Allow is the default view). Each tab will contain both IP and Domain lists of that type.

ThreatBlockr Edge (previously Appliances)

ThreatBlockr Edge Instances (previously Appliances) will be accessed via the Edge Instances sub-menu item under ThreatBlockr Edge in the left-hand navigation menu. This screen will contain the same important information as it did before.

Edge Software

The new Edge Software menu item (which will be under ThreatBlockr Edge in the left-hand navigation) will be where you'll access the automated update controls to update to the latest ThreatBlockr Edge software builds as they are released over time. If any build updates are scheduled or pending, those details will be displayed. Users will continue to have the option to install new builds immediately or schedule an installation for a future date and time.

IPs by ASN (previously ASN Risk Adjustments)

This redesign will include Improvements to the IPS by ASN (previously ASN Risk Adjustments) user experience by removing manual scoring configuration for ASNs. Users will now provide a direct "Block" or "Allow" verdict for each desired ASN.

Post release, any previous ASN Adjustments that had a negative score will have an Allow verdict. Those that had a positive score will have a Block verdict. We recommend you review your IPs by ASN adjustments to make sure the collection of ASN actions makes sense for your environment.

New Features

Protected Networks & Ports (Resource & Service Groups)

We are steadily moving towards a single pane of glass to configure and administer your ThreatBlockr! Users will be able to configure their Protected Networks (known as Resource Groups on the Edge UI) and Protected Ports (known as Service Groups on the Edge UI) in the ThreatBlockr admin console.

An Edge instance will need to have a ThreatBlockr Edge build greater than 180 installed to fully take advantage of these features within the admin console. As such, we strongly urge customers to update to the latest software to be able to use these powerful centralized control features. Customers who do not update will not be able to control these features centrally, and instead must leverage the legacy Edge UI elements.

HELP!

If you find you have questions as you peruse the new interface, don't hesitate to reach out! Our Customer Success team is always ready to assist you in any way.