

PROTECTED THEATER IN THE DIRECTOR

The Director provides control and access to your Protected Theater. Your Protected Theater can be accessed by selecting **Environment > Protected Theaters**. Here, you see everything that is associated with the Protected Theater, including:

- Protected Theaters
- Protected Actors
- Protected Rule Assignments
- Protected Communication Rules
- Protected DNS Rules
- Protected Dynamic Rules
- Protected Rulesets
- Ignored Connections

All aspects of Protected Theater can be configured from this area of the Director user interface.

Protected Theaters

[Add Protected Theaters](#)

Virtual environments to safely test potentially destructive Actions on Protected Actors

Name	Description	Management IP	Test IP	Security Zone	OS	Uptime	Last Comms	Actions

Protected Actors

[Add Protected Actors](#)

Endpoint Actors running inside a Protected Theater

Name	Description	Management IP	Test IP	Security Zone	OS	Uptime	Last Comms	Actions

Protected Rule Assignments

[Add Protected Rule Assignment](#)

Assign protected Communication, DNS, or Dynamic rules to individual Protected Theaters

Assignment ID	Name	Desc	Number of Rules/Rulesets	Number of Protected Theaters	Number of Protected Actors	Actions
1	Installers		10	0	0	
2	protected theater 1		4	0	0	

Protected Communication Rules

[Add Protected Communication Rule](#)

Connections that are allowed from Protected Actors out of the Protected Theater virtual environment and into the real network

Rule ID	Name	Protocol	Destination IP	Destination Port	Actions
7	fileserver	tcp		8000	
3	HX	tcp		443	

Protected DNS Rules

[Add Protected DNS Rule](#)

Define responses for DNS requests made by Protected Actors

Rule ID	Name	Domain	IP Address	Actions

Protected Dynamic Rules

[Add Protected Dynamic Rule](#)

Combination of protected DNS and Communication Rules that automatically resolve and allow communications to the real IP addresses for a domain name

Rule ID	Name	Domain	Protocol	Destination Port	Last Resolved	Refresh Rate	Last Refresh	Actions
1	Director	app.validation.mandiant.com	tcp	443		24	2022-07-27 21:09:09 UTC	
11	Mandiant Login	login.mandiant.com	tcp	443		24	2022-07-27 21:09:09 UTC	

Protected Rulesets

MSV Defined Rulesets for Accessing Specific Assets

Rule ID	Name	Port(s)/Protocol	Domains
1457	FireEye Helix	80,443/TCP	*.fireeye.com, *.apps.fireeye.com, *.ingest.apps.fireeye.com
1566	Mandiant Authentication	443/TCP	app.validation.mandiant.com, login.mandiant.com, mdlogin.fireeye.com, auth.fireeye.com
8	Microsoft Defender	80,443/TCP	*.wdcp.microsoft.com, *.wdcpalt.microsoft.com, *.wd.microsoft.com, *.update.microsoft.com, *.delivery.mp.microsoft.com, *.windowsupdate.com, *.download.microsoft.com, *.download.windowsupdate.com, go.microsoft.com, fe3cr.delivery.mp.microsoft.com, *.blob.core.windows.net, www.microsoft.com, msdl.microsoft.com, vortex-win.data.microsoft.com, settings-win.data.microsoft.com

Ignored Connections

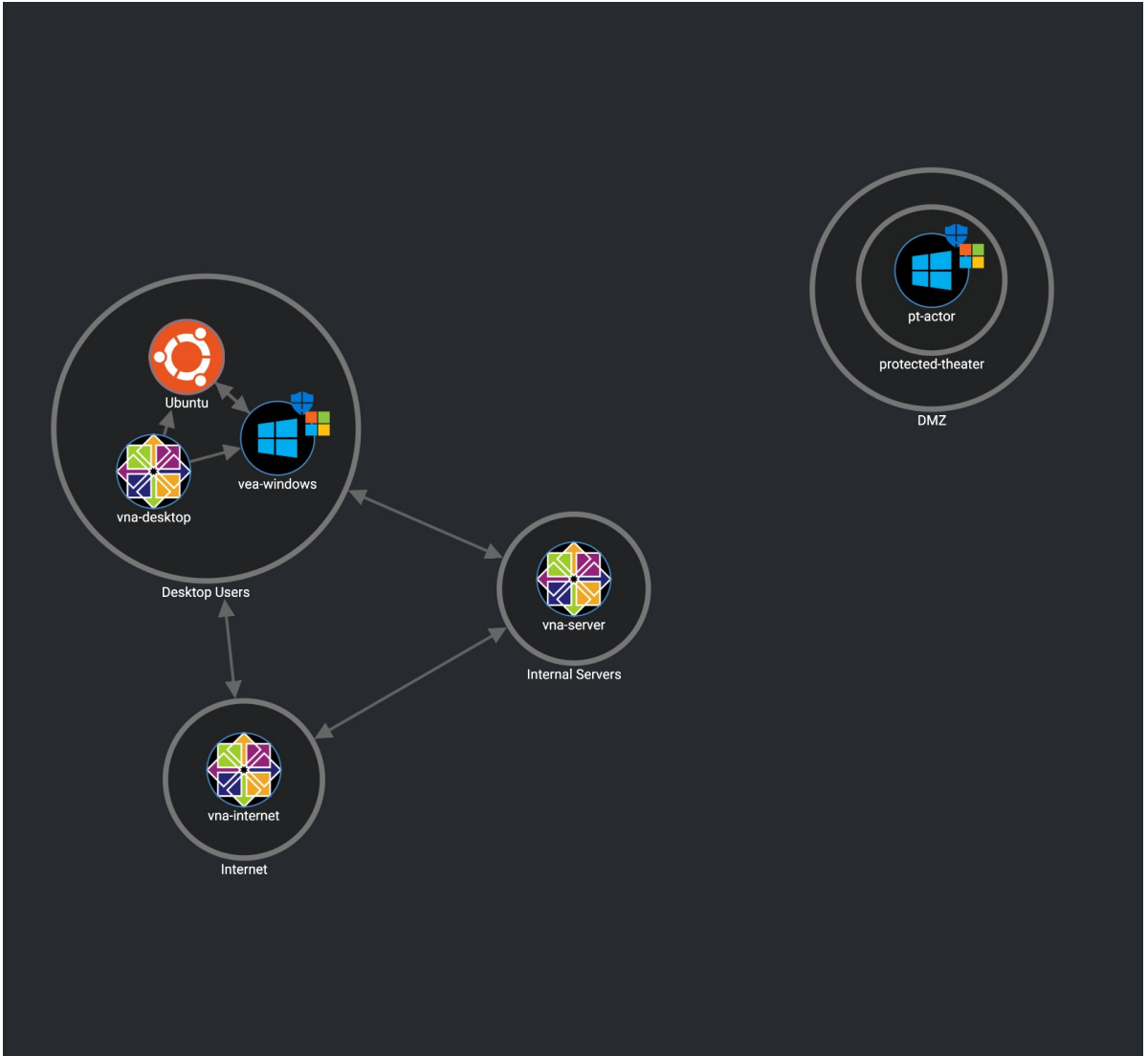
[Add Ignored Connection](#)

Logged connections from Protected Actors that are ignored when determining blocked status

ID	Name	Type	Value	Actions

Protected Theater area in the Director

You also see your Protected Theater on the Environment Map. Access the map by selecting **Environment > Map**. It is also the initial screen you see when you open the Director.



Protected Theater on the map