

F5 Threat Intelligence Agent

Microsoft Security Copilot

Product brief

F5 tracks the evolution of cybersecurity threats across the Open-Source Threat Intelligence (OSINT) landscape. The resulting data is structured and enriched with key information, summarizations, narratives, commentaries, and actionable insights.

Among various use-cases, F5 leverages the insights from the Threat Intelligence data to generate a weekly 'F5 Threat Report' which can be delivered, on request, via email, and it is made available on the [F5 Dev Central portal](#). See one instance of it [here](#).

We are now making the weekly 'F5 Threat Report' conveniently accessible as a Microsoft Security Copilot Agent plugin.

The Agent plugin will initially be made available on the [Microsoft Security Store](#). Customers and Partners will be able to provision the Security Copilot Agent plugin directly in their Security Copilot Workspace of choice and start using it right away.

Functionality

The F5 Threat Intelligence Agent for Microsoft Security Copilot delivers a summarized version of the weekly 'F5 Threat Report'. The full-length threat report is posted weekly on [F5's Dev Central portal](#).

The threat report is generated by combining the Open-source threat intelligence (OSINT) that F5 tracks based on the available, public cybersecurity web sources and blog posts.

As the information from the OSINT sources is processed, key indicators are extracted from the sources and enrich the final data model. Some of the key information include:

1. Vulnerability CVEs IoCs¹
2. Malware Hashes IoCs
3. Malware names
4. Attacking URL
5. Attacking Domain
6. Attacking Ips
7. Attacking Geographies (Country)


¹ Indicator of Compromise

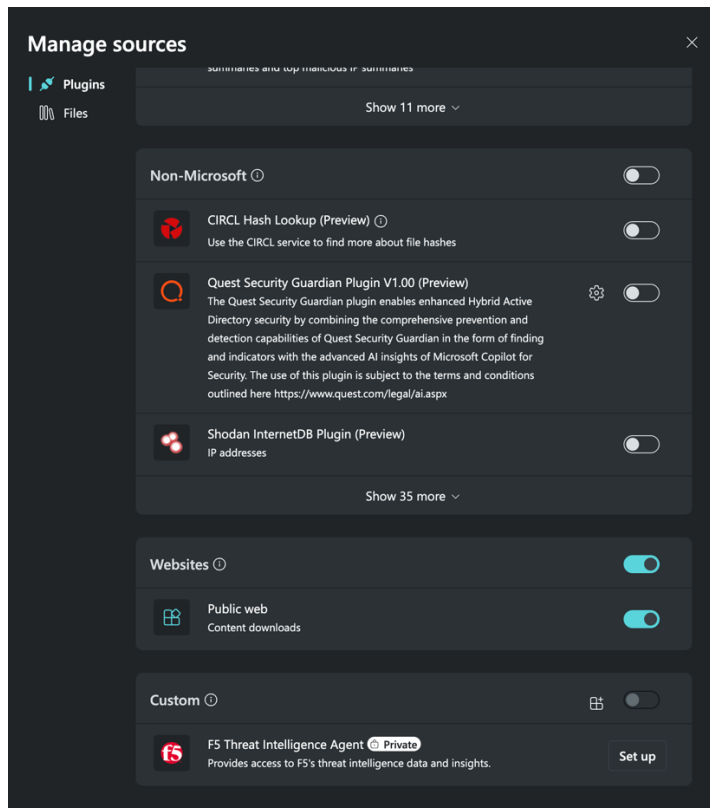
8. Impacted Technologies
9. Impacted Industries
10. Impacted Geographies (Country)

The data is also enriched with summarizations, narratives, commentaries, and actionable insights that are regularly updated as more information about any given threat is sourced.

The plugin can be easily provisioned into your Security Copilot Workspace from the [Microsoft Security Store](#) portal.

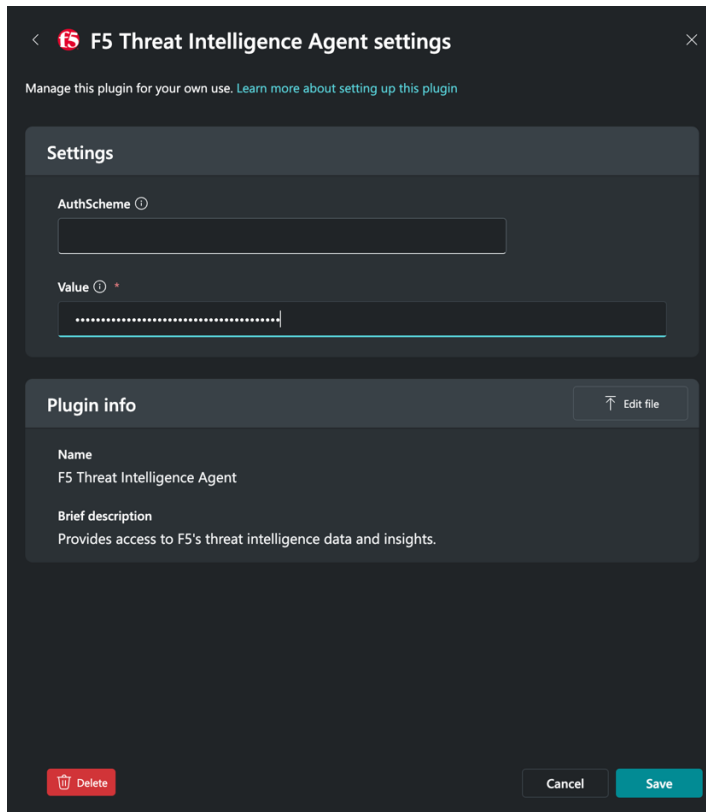
Once provisioned, a Copilot user with the ‘Security Admin’ role² will be able to configure the plugin. The configuration requires an API key, which can be obtained by contacting F5 at azureteam@f5.com. The setup steps are:

1. Open the ‘Sources’ panel by clicking on the  icon on the right-hand side of the chatbot’s input box. This will open a modal window like the following:



² Or a delegate having been given the permission to manage plugin sources.

2. Click the 'Set up' button. You will navigate to the F5 Threat Intelligence Agent's setup screen.



< **F5 Threat Intelligence Agent settings** ×

Manage this plugin for your own use. [Learn more about setting up this plugin](#)

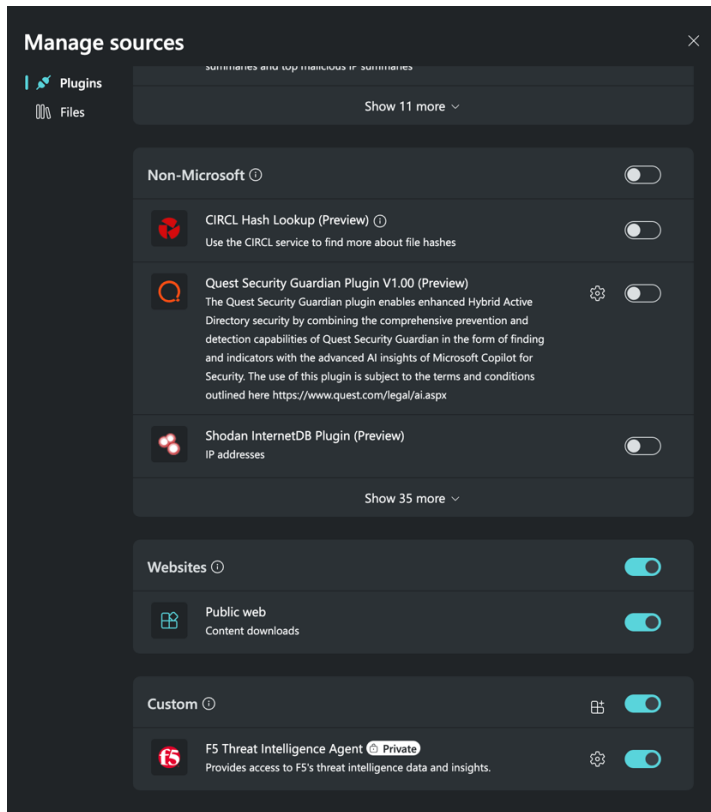
Settings

AuthScheme ⓘ

Value ⓘ *


- a. Leave the 'AuthScheme' input empty.
- b. Add the API key to the 'Value' input.
- c. Click 'Save'.

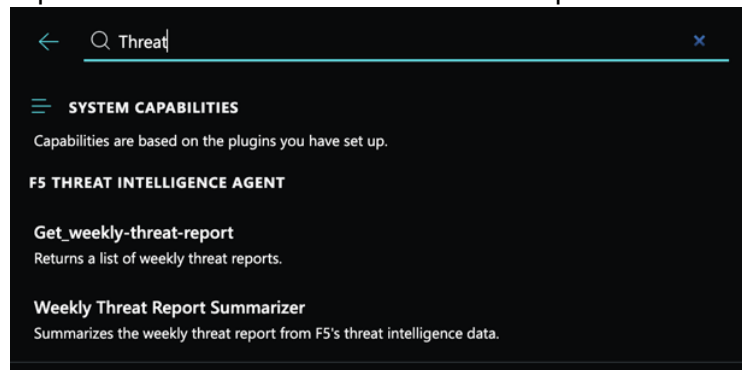
3. Afterwards, the 'F5 Threat Intelligence Agent' plugin in the 'Sources' modal window will look like this:



At this point you will be ready to take the F5 Threat Intelligence Copilot Agent for a spin.

You can do so in two ways:

1. Direct prompt invocation
 - a. On the right-hand side of the chatbot's input box, click on the 'Prompts' icon . A modal screen will open.
 - b. Click on the 'See all system capabilities' shortcut.
 - c. Input 'Threat' in the search box at the top of the screen:



- d. Click on 'Weekly Threat Report Summarizer'.
This will add the prompt to the chatbot's input box.
 - e. No other input required: just press the send button on the right-hand side of the input box.
2. Prompting
- a. Input 'Weekly Threat Report Summarizer' in the chatbot's input box.
 - b. Press the send button on the right-hand side of the input box.

Security Copilot will create a new session and execute the F5 Threat Intelligence Agent. When it's done processing the data, Security Copilot will deliver a pre-formatted, summarized version of the weekly 'F5 Threat Report. It will look as follows:

Microsoft Security Copilot | SecurityCopilot_Workspace | My sessions / Weekly Threat Report Summarizer | Share

Weekly Threat Report Summarizer

> 3 steps completed 49 seconds

Sep 16, 3:47 PM

The weekly threat report highlights five critical security incidents that emerged between August 8 and August 27, 2025:

AI-generated content may be incorrect. Check it for accuracy. Export to Excel

Threat	CVEs	Severity
Docker Desktop Vulnerability	CVE-2025-9074	CRITICAL (9.3)
NVIDIA NeMo Curator RCE	CVE-2025-23307	CRITICAL (7.8)
s1ngularity Supply Chain Attack	N/A	CRITICAL
Citrix NetScaler Zero Days	CVE-2025-7775, CVE-2025-7776, CVE-2025-8424, CVE-2025-6543	CRITICAL (up to 9.2)

This summary covers incidents reported in the last three weeks and includes five major threats.

How can Security Copilot help?

AI-generated content may be incorrect. Check it for accuracy.