Web Security Cloud

2023

Release Notes

Revision A

Contents

Introduction

This document details product updates and new features added to Forcepoint Web Security Cloud during 2023.

What's new?

New categories related to Artificial Intelligence (AI) and Machine Learning (ML) added

New categories related to AI and ML are added to the existing set of categories used by the Forcepoint URL Database.

Four new sub categories are added within the "**Information Technology**" parent category for easy and fine-grained policy management.

Customers can get more benefits and protect themselves against the potential risks coming with the game changing innovations happening in the field of AI and ML technologies.

The new categories are listed below:

Category Name	Description
Other AI ML Applications	Sites that provide tools or services related to AI and ML. Includes sites hosting applications with personal productivity or business purposes using AI but not typically capable of generating new content.

Category Name	Description
Generative AI – Multimedia	Sites that specialized in machine-generated multimedia content such as images, videos, or audios. Includes sites that provide information, tools, or services related to text-to-speech, video, music, sound, or image editing applications using AI with the ability to generate new content.
Generative AI - Conversation	Sites that specialized in machine-generated conversational content for the purpose of general information, user assistance, or entertainment. Includes sites hosting virtual agents and limited domain conversational applications using AI with the ability to generate new content.
Generative AI - Text & Code	Sites that provide machine-generated text with large domain applications (including code and translation) using AI and generating new content. Includes sites that provide tools or services that make suggestions, edits, reviews, or create summaries based on the user prompts and interactions.

Forcepoint Single Sign-On (SSO) metadata updated for Web Security Cloud

The digital certificate used by Forcepoint to authenticate **end-users** using SSO has been updated, as the previous certificate expires on September 13th, 2023, 23:59 UTC.

SSO requests will fail for any customers who will use the old certificate after this time and end-users will not be able to use the service.

Important

If you are using the SSO feature for **end-users**, you must take immediate action to ensure the Forcepoint metadata used by your Identity Provider (IdP) is up-to-date.

- If you point your IdP to the Forcepoint metadata URL, no action is required.
- If you have downloaded a local copy of Forcepoint metadata for use by your IdP, you must download the new metadata and import it to your IdP.

A technical alert email has already been sent to the service administrators. Full details of the alert and instructions for the actions to take can be found in this knowledge base article.

Increased the list length of application bypass entries

From the **22.04.0.2809 newer Neo Endpoints version**, it is possible to add additional application bypass entries up to the total list length of 3840 characters. Microsoft and Mac applications appear on separate tabs for ease of use.

List length for earlier Neo Endpoints and all Classic Endpoints is unchanged with 1920 characters. This change has no impact on the existing Endpoint application bypass configurations.

Adding Analysis exceptions with the hostname and path

While adding Analysis Exceptions, it is possible to specify the hostname and path that allows more granular exceptions to be configured.

This change has no impact on the existing Analysis Exception configurations.

New filter added in File Sandboxing Report

File not supported filter added in the File Sandboxing Report. This filter option detects a file which was not supported by the Advanced Malware Detection module.

End user facing texts aligned with Forcepoint Inclusive Language Standards

All end user texts used in Forcepoint Cloud Security Gateway Portal have been aligned to use words as per Forcepoint Inclusive language guidelines.

Security Enhancements

There is an on-going effort to improve the security of Forcepoint products. To that end, Forcepoint Security Labs Analysts continually assess potential security vulnerabilities which can be introduced by third-party libraries. Security improvements have been made in several areas.

Description	References	Date
In the Forcepoint CSG Portal, improper neutralization of the special elements used in the SQL command (SQL Injection Vulnerability) allows a blind SQL injection on the Web Security Cloud and Email Security Cloud in certain circumstances.	Blind SQL Injection Vulnerability	12-Jun-2023
Improper handling of input during generation of a web page	Cross-site Scripting (XSS) vulnerability	29-Mar-2023

Previous updates

For details of new features added, and issues resolved during 2022, 2021, 2020, and 2019, see the Forcepoint Web Security Cloud 2022 Release Notes, Forcepoint Web Security Cloud 2021 Release Notes, Forcepoint Web Security Cloud 2020 Release Notes, Forcepoint Web Security Cloud 2019 Release Notes.

Resolved and known issues

There are no resolved and known issues in this release. To see the latest list of resolved and known issues for Forcepoint Web Security Cloud, see Resolved and known issues for Forcepoint Web Security Cloud - 2023 in the Forcepoint Knowledge Base.

You must log on to the Customer Hub to view the list.

Limited availability features

The table below lists Forcepoint Web Security Cloud features that are in a limited availability status. Limited availability features may have been released recently, or may need to be approved by your account manager before being added for your organization, due to additional configuration requirements, or other considerations.

If you are interested in enabling any of these features for your account, please contact Technical Support.

Feature	Description
Acceptable use policy	Allows administrators to require that end users periodically accept the terms of an acceptable use policy (AUP) before continuing to browse via the proxy. The feature can be set per policy, and users are required to accept the AUP every 1, 7, or 30 days. The AUP confirmation screen can be customized under **Web** > **Policy Management** > **Block & Notification Pages**. For further information, see the Forcepoint Security Portal Help.
Password policy for end users	Allows you to apply the same password policy requirements both for administrators accessing the cloud portal, and end users manually authenticating with the proxy. Password policy settings are configured on the **Account** > **Contacts** page. For further information, see the Forcepoint Security Portal Help.

Feature	Description
Full traffic logging	Allows administrators to download full fixed format web traffic logs for retention and analysis, which can be useful for integration with third-party SIEM tools. Logs can be downloaded for 14 days and are provided in JSON format. For further information, see Configuring Full Traffic Logging on the Forcepoint Support website. Forcepoint recommends using the more recent and more flexible SIEM Integration option. Take advantage of Bring your own storage for closer SIEM tool integration or switch between Forcepoint storage and your own See Configuring SEIM storage in Web Security Cloud Help.
Remote Browser Isolation	Send blocked web requests to a third-party remote browser isolation provider, allowing the web page to be viewed outside of the organization's network. For further information, see Configure Remote Browser Isolation in the Security Portal Help.

Published 08 August 2024