

COMGUARD



Skyhigh Security Service Edge

In Practice - Security & AI

September 2023

Nino Tolić, Systems Engineer



We protect the world's data

- Data-first security protection enabling information sharing without impacting the user experience
- The most advanced Security Service Edge data protection available
- Single security platform that is simple to use with the fastest time to value

2023 Gartner® Magic Quadrant for Security Service Edge



2023 Gartner® Critical Capabilities for Security Service Edge

Skyhigh Security is rated as excellent and was the highest scoring vendor in two out of four use cases in this research.

End users looking for a comprehensive SSE solution should use Skyhigh Security.

Secure Web and Cloud Usage	#1
Detect and Mitigate Threats	#1
Connect and Secure Remote Workers	#3
Identify and Protect Sensitive Information	#3



3000+ Customers
80% of Global Banks
25% of Fortune 500



Gartner.
Peer Insights™

Skyhigh Security Rated 4.7/5

based on 763 reviews
in the Security Service Edge market



as of 1/24/2023

★★★★★ October 21, 2022

Product: Skyhigh Security SSE

"Pervasive Data Protection Anywhere"

"We found the Skyhigh security SSE solution to be feature rich, the cloud web and on-prem hybrid integration helped me protect and meet the data protection objective of my enterprise security. The flexibility of DLP and single panel for CASB/SWG/RBI & ZTNA is..."

[Read Full Review >](#)

Disclaimer: The Gartner Peer Insights Customers' Choice badge is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner Peer Insights Customers' Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates.

Skyhigh Security



Security Service Edge Portfolio

Additional Products

SWG



Skyhigh
Secure Web Gateway

CASB



Skyhigh
Cloud Access Security Broker

ZTNA



Skyhigh
Private Access

CNAPP



Skyhigh
CNAPP

FWaaS



Skyhigh
Cloud
Firewall

ENDPOINT



Trellix
DLP

DATA PROTECTION



Skyhigh
Cloud Platform

Advanced Data Loss Prevention · Intuitive Dashboard · Advanced Browser Isolation · AI / ML
Unified Client · Unified Policy Management · Unified Threat Prevention · Unified Incident
Management

Growth of AI Services

Examples of AI services



ChatGPT (OpenAI)

Can you write me a coda.io formula that checks all rows inside a table to see if the status is complete or not

Sure, here is a coda.io formula that you can use to check all rows in a table to see if the status is complete:

```
=COUNTIF([Status], "Complete")
```

This formula will count all rows in the table where the value in the "Status" column is "Complete". You can modify the formula to suit your specific needs, such as checking for a different status value or using a different column.

Here is an example of how you might use this formula in a table:

Task	Status
Write report	In progress
Submit report	Complete
Review report	In progress
Approve report	In progress

To check if any rows in the table have a value of "Complete", you would use the

ChatGPT is optimized for dialogue. Our goal is to make AI systems more natural to interact with, and your feedback will help us improve our system.

Bard (Google)

I'm Bard, your creative and helpful collaborator. I have limitations and won't always get it right, but your feedback will help me improve.

Not sure where to start? You can try:

- Outline my blog post about summer mocktail recipes
- Help me incorporate more high-protein vegan options in my diet
- Help me finish my art studio tagline: craft, create, and ...

briefly tell me what you can do

Bard may display inaccurate or offensive information that doesn't represent Google's views.

Bing Chat (Microsoft)

Welcome to the new Bing

Your AI-powered copilot for the web

- Ask complex questions
- Get better answers
- Get creative inspiration

Let's learn together. Bing is powered by AI, so surprises and mistakes are possible. Make sure to check the facts, and share feedback so we can learn and improve!

bing AI

Jasper

Write a blog post about the benefits of vegetables. Include references to sources.

Vegetables are an essential part of a healthy diet. Not only do they provide essential vitamins, minerals, and other nutrients, but they also offer many health benefits. Eating vegetables every day can help protect your eyes and skin, accelerate the process of healing cuts and wounds, help absorb iron better, and in weight management, and even improve your gut microbiome.

When it comes to improving your overall health, there are few things more important than eating plenty of vegetables. Here are just a few of the many benefits that come with eating vegetables:

- Fight inflammation:** Vegetables contain antioxidants that can help reduce inflammation in the body. This can lead to improved cardiovascular health and better overall wellbeing.
- Improve blood pressure:** Eating plenty of vegetables can help lower blood pressure levels by reducing sodium intake.

Write a country song about cats in the style of Willie Nelson

Write a tweet from the CEO of Twitter introducing the new Twitter Blue subscription.

Introducing Twitter Blue! Our first-ever subscription offering that lets you customize your Twitter experience with access to exclusive features and perks. Try out our "Undo Tweet" button, a Nuzzel-like "Top Stories" feature, ad-free articles, and more - all for just \$2.99/month. Get your Tweet on and sign up for Twitter Blue now! #TwitterBlue

Create images of the most beautiful place in the world

Can you help me write a Facebook ad copy for promoting Writesonic?

Chatsonic (Writesonic)

Skyhigh Security SSE Customer Telemetry



650+

Shadow Services
Cloud Registry



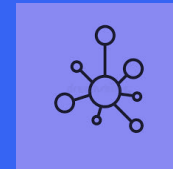
~30

High Risk AI Services



1TB+

Data Uploaded



215M+

Total Connection
Requests

Sample Customer Data Overview



Services

Year to Date Jan 1 - Jun 21 UTC

Service Sub-Category: Artificial Intelligence

Save View

Service Group

- Unassigned 78
- Upload-Blocked 3
- Blocked 3
- ITAR 2

Permission Type

- Allowed 85
- Denied 26

Risk Attributes

Select an attribute ▼

Risk Type

Service Usage

Service Status

Service Category

Location

Tag Type

User/IP Address Type

Data

Device Type

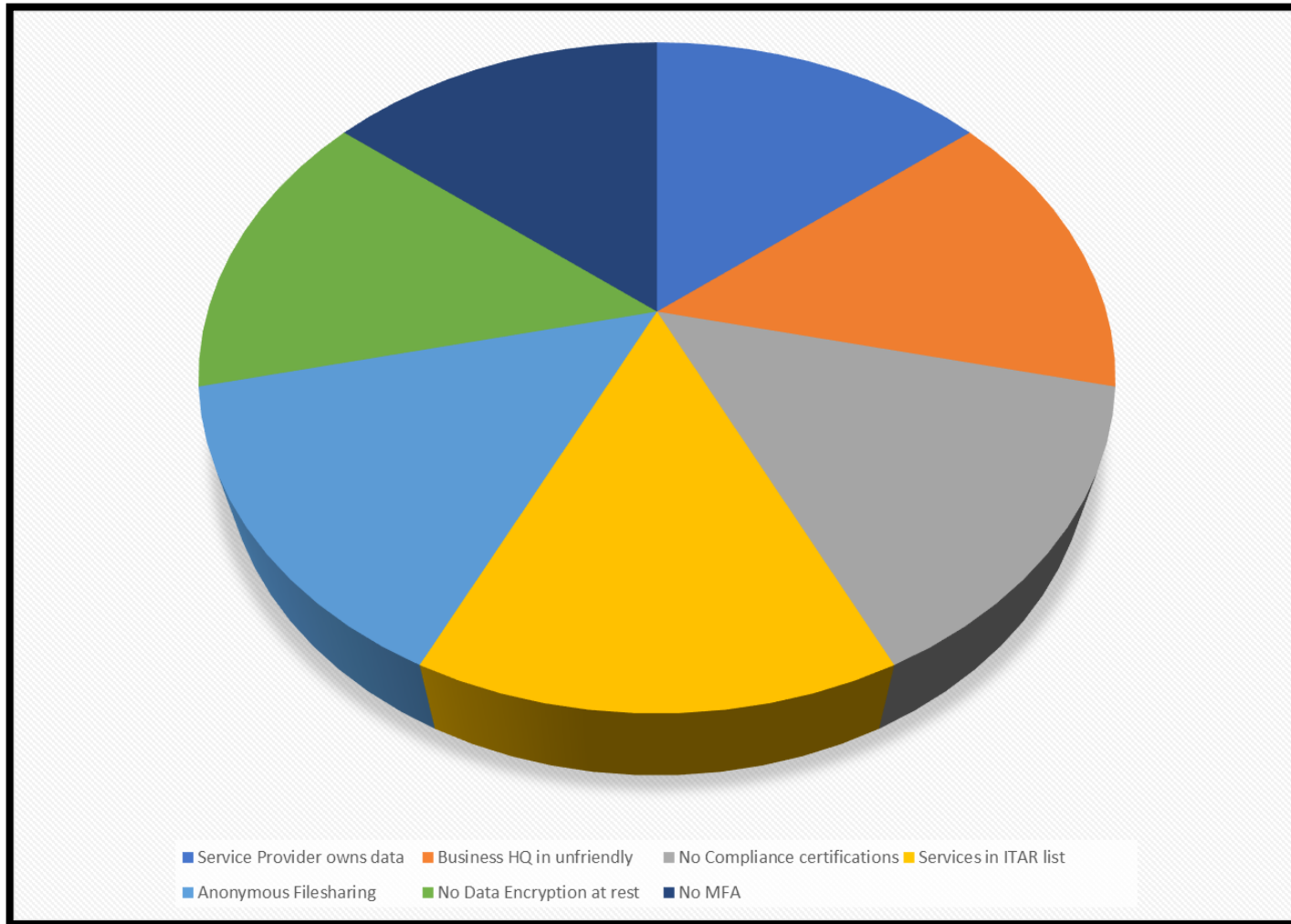
Hosted on Third-Party Services

86 Services

<input type="checkbox"/>	Risk	Service Name	Category	Service Group(s)	Users	Upload Activities	Upload Data	Inbound Data	Outbound Data	Allowed Requests	Denied Requests
<input type="checkbox"/>	6	OpenAI - ChatGPT	Artificial Intelligence	Unassigned	1,905	86.3 k	21 GB	31.2 GB	23.8 GB	884.9 K	1,060
<input type="checkbox"/>	5	Bing New (Bing Chat)	Artificial Intelligence	Unassigned	6,036	292.5 k	6 GB	35.9 GB	26.6 GB	7.2 M	23.5 K
<input type="checkbox"/>	6	You - YouChat	Artificial Intelligence	Unassigned	15	1,962	20.4 MB	48.8 MB	83.4 MB	16.4 K	11
<input type="checkbox"/>	5	Wordtune	Artificial Intelligence	Unassigned	19	488	8 MB	252 MB	25.8 MB	5,190	8
<input type="checkbox"/>	3	Boost AI	Artificial Intelligence	Upload-Blocked	56	22	6.6 MB	74.2 MB	8.4 MB	2,607	17
<input type="checkbox"/>	5	OpenAI - DALL-E 2	Artificial Intelligence	Unassigned	81	5	4.9 MB	1.4 MB	6.3 MB	1,292	1
<input type="checkbox"/>	5	Sardine	Artificial Intelligence	Unassigned	2	4	4.7 MB	1.5 MB	4.9 MB	567	1
<input type="checkbox"/>	5	Tome	Artificial Intelligence	Unassigned	15	249	2.9 MB	46 MB	7.7 MB	3,231	8
<input type="checkbox"/>	5	Zoovu	Artificial Intelligence	Unassigned	29	202	2.4 MB	10.8 MB	6.7 MB	3,535	4
<input type="checkbox"/>	6	DataMilk	Artificial Intelligence	Unassigned	47	133	2.3 MB	3.9 MB	7.1 MB	2,747	2
<input type="checkbox"/>	2	UiPath	Artificial Intelligence	Unassigned	11	66	1 MB	96.9 MB	12.1 MB	2,813	1
<input type="checkbox"/>	6	Google Bard	Artificial Intelligence	Unassigned	87	76	1 MB	11 MB	11.7 MB	5,497	4
<input type="checkbox"/>	6	muse.ai	Artificial Intelligence	Unassigned	6	1	999.3 KB	5.1 MB	1.1 MB	134	0
<input type="checkbox"/>	2	Cisco - AI Network Analytics	Artificial Intelligence	Unassigned	36	67	632.6 KB	106.5 MB	16.9 MB	4,849	0
<input type="checkbox"/>	4	Hugging Face	Artificial Intelligence	Unassigned	18	3	479.6 KB	29.2 MB	6.3 MB	6,248	2
<input type="checkbox"/>	6	PDF Chatbot	Artificial Intelligence	Unassigned	4	1	253.7 KB	6.1 KB	254.8 KB	4	0
<input type="checkbox"/>	5	Increasingly	Artificial Intelligence	Unassigned	48	1	250 KB	467.7 KB	938.1 KB	854	0
<input type="checkbox"/>	5	Black Crow AI	Artificial Intelligence	Unassigned	104	5	73 KB	5.7 MB	2.6 MB	2,963	15
<input type="checkbox"/>	6	Gamma	Artificial Intelligence	Unassigned	5	1	24.9 KB	10.1 MB	5.4 MB	4,401	9
<input type="checkbox"/>	6	Google - Quick, Draw!	Artificial Intelligence	Unassigned	4	2	19.5 KB	1.1 MB	130.1 KB	66	0
<input type="checkbox"/>	4	Cognigy	Artificial Intelligence	Unassigned	2	1	16.8 KB	19.9 KB	21.9 KB	9	0

Protecting AI Services

AI Services - Common Risks & Pain Points



1. Lack of visibility and control - Which AI services are being used?. Without visibility you cannot exercise any control over these AI chatbots, which means being blind to their risks.
2. Protecting sensitive, confidential, and business critical data - Everyone wants to use AI services, but at the risk of losing proprietary and sensitive information?

How to Enable the benefits of AI Services rather than saying "NO"



Premium HOME > TECH

Amazon warns employees not to share confidential information with ChatGPT after seeing cases where its answer 'closely matches existing material' from inside the company

Eugene Kim Jan 25, 2023, 9:15 AM GMT+11



BREAKING

JPMorgan Chase Restricts Staffers' Use Of ChatGPT

Siladitya Ray Forbes Staff
Covering breaking news and tech policy stories at Forbes.

Follow

Feb 22, 2023, 07:21am EST

Listen to article 2 minutes



TOPLINE JPMorgan Chase has restricted the use of ChatGPT by its staff, Bloomberg and the *Telegraph* reported, becoming the latest organization to limit the use of OpenAI's chatbot in the workplace following the likes of Amazon and several U.S. universities.

Mar 11, 2023 - Technology

Companies are struggling to keep corporate secrets out of ChatGPT

Sam Sabin, author of [Axios Codebook](#)

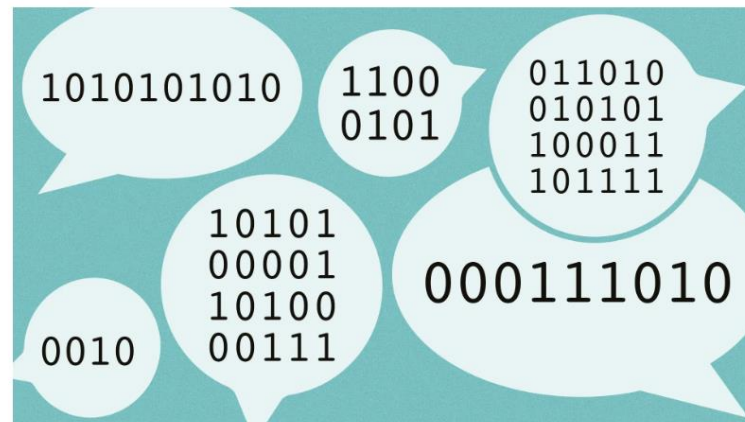


Illustration: Shoshana Gordon/Axios

FORBES > BUSINESS

BREAKING

Samsung Bans ChatGPT Among Employees After Sensitive Code Leak

Siladitya Ray Forbes Staff

Covering breaking news and tech policy stories at Forbes.

Follow

May 2, 2023, 07:17am EDT

Listen to article 3 minutes



Updated May 2, 2023, 07:31am EDT

TOPLINE Samsung Electronics has banned the use of ChatGPT and other AI-powered chatbots by its employees, Bloomberg reported, becoming the latest company to crack down on the workplace use of AI services amid concerns about sensitive internal information being leaked on such platforms.



How Skyhigh Security protects sensitive data in AI Services?



1. Gain granular visibility and control into which AI Chatbots are being used in the company from managed devices

- a. Which AI apps are available today

Cloud Registry

Filters Views Service Category: Artificial Intelligence Save View

Service Category

- Media 695
- Project Management 657
- Artificial Intelligence 651
 - Artificial Intelli... 651
- e-Commerce 564
- CRM 528
- Cloud Storage 512
- Networking 451

Risk Type

- High Risk
- Low Risk
- Medium Risk

Cloud Services

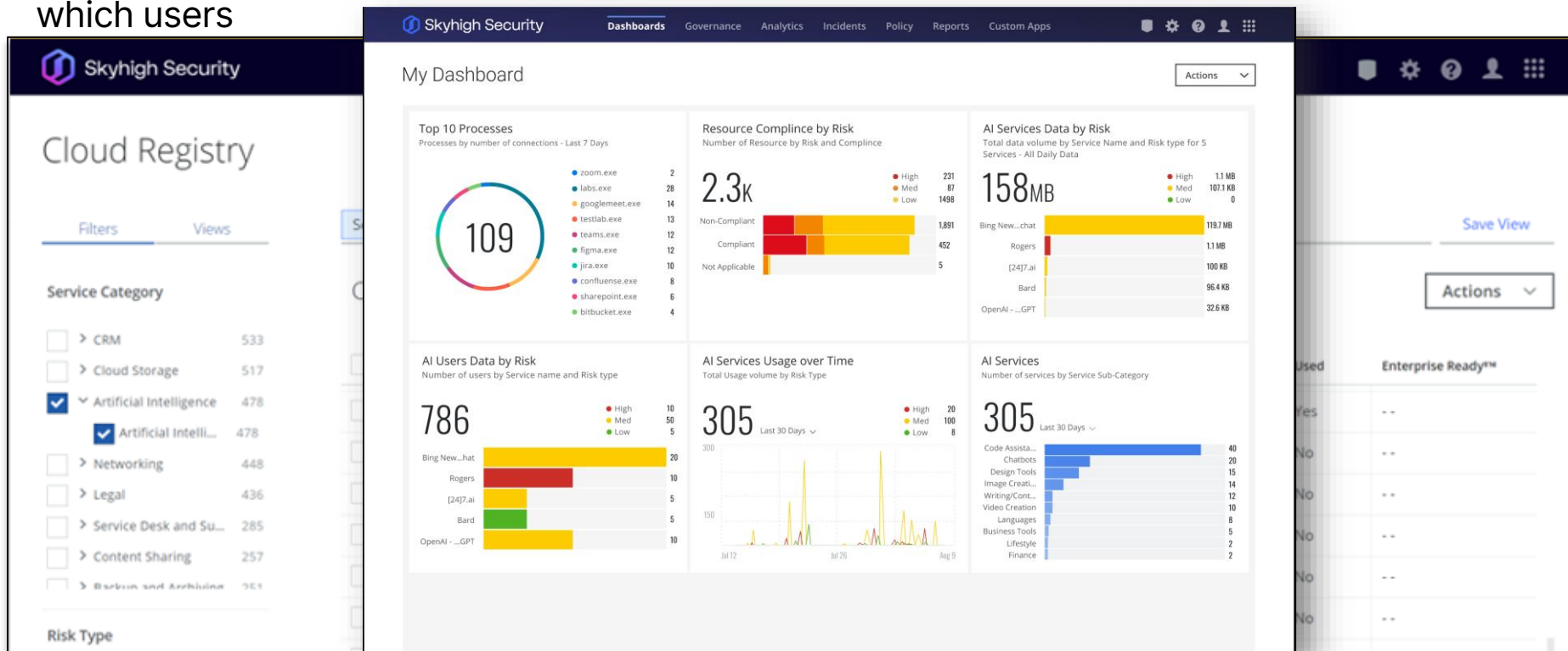
Actions

<input type="checkbox"/>	Risk	Service Name	Category	Subcategory	Service Group(s)	Used ↓	Enterprise Ready™
<input type="checkbox"/>	5	[24]7.ai	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU GL	Yes	--
<input type="checkbox"/>	4	LivePerson AI	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU GL	Yes	--
<input type="checkbox"/>	6	OpenAI - ChatGPT	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU GL	Yes	--
<input type="checkbox"/>	6	Bing New (Bing Chat)	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU GL	Yes	--
<input type="checkbox"/>	4	Vidado (Formerly Captricity)	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU GL	No	--
<input type="checkbox"/>	7	Brevity AI	Artificial Intelligence	Artificial Intelligence	High Risk Services, C	No	--
<input type="checkbox"/>	4	Lionbridge	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU GL	No	--
<input type="checkbox"/>	4	PROS	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU GL	No	--
<input type="checkbox"/>	6	iFLYTEK Open Platform	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU GL	No	--
<input type="checkbox"/>	6	Now Interact	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU GL	No	--

How Skyhigh Security protects sensitive data in AI Services?



1. Gain granular visibility and control into which AI Chatbots are being used in the company from managed devices
 - a. Which AI apps are available today
 - b. Discover which AI Apps are being used by which users



How Skyhigh Security protects sensitive data in AI Services?



1. Gain granular visibility and control into which AI Chatbots are being used in the company from managed devices
 - a. Which AI apps are available today
 - b. Discover which AI Apps are being used by which users
 - c. Know about the amount of data being uploaded to each app

Services All Daily Data Apr 17 - Jun 7 UTC

Filters Views Service Group: AI Warning Save View

Service Group: AI Warning 4 Services Actions

	Risk	Service Name	Category	Subcategory	Service Group(s)	Users	Upload Data	Inbound Data	Outbound Data	Allowed Requests	Denied Requests	Service First Used
<input type="checkbox"/>	6	OpenAI - ChatGPT	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU	2	15.7 kB	3.8 kB	17.7 kB	4	3	May 31, 2023 UTC
<input type="checkbox"/>	4	Rogers	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU	4	2.1 MB	25.6 MB	7.3 MB	341	0	May 26, 2023 UTC
<input type="checkbox"/>	6	Bing New (Bing Chat)	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU	794	7.2 MB	94.9 MB	25.7 MB	26.5 K	0	Apr 28, 2023 UTC
<input checked="" type="checkbox"/>	5	[24]7.ai	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU	2	60.8 kB	132 kB	90 kB	31	0	Nov 01, 2017 UTC

How Skyhigh Security protects sensitive data in AI Services?



1. Gain granular visibility and control into which AI Chatbots are being used in the company from managed devices
 - a. Which AI apps are available today
 - b. Discover which AI Apps are being used by which users
 - c. Know about the amount of data being uploaded to each app
 - d. Block risky AI Apps
 - e. Block some activities (login, upload) in specific AI chatbots

The screenshot shows the 'Web Policy' configuration page in Skyhigh Security. The left sidebar contains a navigation menu with 'Application Control' highlighted. The main content area is titled 'Activity Control New 1' and shows a list of rules. A red box highlights the 'AI Warning: Select Activities to Block' checkbox, which is currently unchecked. Below this, there are three sections: 'Service Groups (1)', 'Service Category (3)', and 'Individual Services (1)'. The 'Service Category (3)' section has three checked items: 'Content Sharing (All): Upload', 'IaaS Admin Console (All): Login', and 'Development (1/7): Login'. The 'Individual Services (1)' section has one checked item: 'Bebo: Photo share Post'. At the bottom of the sidebar, 'Activity Control New 1' is also highlighted with a red box.

How Skyhigh Security protects sensitive data in AI Services?



1. Gain granular visibility and control into which AI Chatbots are being used in the company from managed devices
 - a. Which AI apps are available today
 - b. Discover which AI Apps are being used by which users
 - c. Know about the amount of data being uploaded to each app
 - d. Block risky AI Apps
 - e. Block some activities (login, upload) in specific AI chatbots
2. Protect sensitive and confidential data from getting leaked/exposed.
 - a. Coach users on the risks of using AI chatbots

The screenshot displays the configuration interface for 'Web Filtering Coach URLs'. On the left, a table lists criteria for coaching sessions:

Name	Criteria	Operator	Value
Category & Domain Coaching	IF All Traffic	-	-

Below the table, there are preset rules and coaching options:

- Set coaching session timeout to 30 Min
- Coach & Allow access to these categories
- Coach & Allow access to these domains

On the right, the 'Web Filtering Coach URLs' section includes an 'Add description' field, an 'Actions' dropdown, and a table for coaching URLs:

Smart Match	Comment
https://openai.com/	
https://openai.com/blog/chatgpt	

How Skyhigh Security protects sensitive data in AI Services?



1. Gain granular visibility and control into which AI Chatbots are being used in the company from managed devices
 - a. Which AI Apps are available today
 - b. Discover which AI Apps are being used by which users
 - c. Know about the amount of data being uploaded to each app
 - d. Block risky AI Apps
 - e. Block some activities (login, upload) in specific AI Apps
2. Protect sensitive and confidential data from getting leaked/exposed.
 - a. Coach users on the risks of using AI Apps
 - b. Apply DLP policies to allowed AI Apps

Web DLP

This rule set blocks the transfer of sensitive information outside your organization's network based on DLP Classifications that McAfee maintains and that you can configure.

! Scope DLP Policies individually.

Global Downselection Settings

File types to exclude from Web DLP evaluation ...

Limit processing the files less than MB

DLP Policies

<input type="checkbox"/>	Source Code	keven_how...	Jan 31, 2022 UTC
<input checked="" type="checkbox"/>	AIP	keven_how...	Aug 12, 2021 UTC
<input checked="" type="checkbox"/>	SSN_PII Governance Policy	keven_how...	May 3, 2022 UTC
<input checked="" type="checkbox"/>	PCI	keven_how...	Feb 24, 2022 UTC
<input checked="" type="checkbox"/>	HIPAA	keven_how...	Mar 3, 2021 UTC
<input checked="" type="checkbox"/>	Confidential Governance Policy	keven_how...	May 18, 2021 UTC
<input checked="" type="checkbox"/>	Block sensitive data from IP ownership sites	keven_how...	Dec 16, 2020 UTC

How Skyhigh Security protects sensitive data in AI Services?



1. Gain granular visibility and control into which AI Chatbots are being used in the company from managed devices
 - a. Which AI Apps are available today
 - b. Discover which AI Apps are being used by which users
 - c. Know about the amount of data being uploaded to each app
 - d. Block risky AI Apps
 - e. Block some activities (login, upload) in specific AI Apps

2. Protect sensitive and confidential data from getting leaked/exposed.
 - a. Coach users on the risks of using AI Apps
 - b. Apply DLP policies to allowed AI Apps
 - c. Force Disable Chat History and Training
 - d. Disable copy from Clipboard
 - e. Limit the amount of data uploads Force
 - f. Prevent sharing of Conversation History



<https://www.skyhighsecurity.com/about/resources/demos/skyhigh-web-gateway-interactive-demo-for-ai-applications.html#demo-anchor>

** Available via Custom Rule Set – coming soon within product*

Skyhigh SSE Hands-On Workshop



- Join us in our next 3 hour SSE Hands-On Workshop and setup and try Skyhigh yourself:

Join Skyhigh Security for our interactive SSE Hands-On Workshops - created specifically for technology specialists and customers with existing experience in our Web Gateway solution to get to know our cloud-based SSE solution through a unique experience.

In this three-hour workshop, you will learn the following technologies in your own provisioned account under the guidance of Skyhigh System Engineers, and will be able to try out the following solutions and capabilities:

Secure Web Gateway (SWG)

Configure web policies from the cloud.

Cloud Application Control (CASB)

Control access to and activities in cloud services from a comprehensive cloud registry.

Remote Browser Isolation (RBI)

Allow access to unknown or potentially dangerous websites without exposing your client to malicious code.

Data Loss Prevention (DLP)

Prevent improper storage and/or transmission of sensitive information.

Private Access (ZTNA)

Allow secure access to internal corporate resources without the need for a VPN client.

Register here:

<https://www.skyhighsecurity.com/sse-virtual-workshop>





Thank You!

www.skyhighsecurity.com