

Configureer Private ChatGPT en beperk de toegang tot andere generatieve AI-apps

Inhoud

[Inleiding](#)

[Overzicht](#)

[Stap 1: Maak een webregel om uw privéchat-gpt toe te staan](#)

[Stap 2: Blokkeer alle andere generatieve AI-apps](#)

[DNS-beleid](#)

[webbeleid](#)

Inleiding

In dit document wordt beschreven hoe u een privé ChatGPT kunt configureren en de toegang tot andere generatieve AI-apps kunt beperken.

Overzicht

Het landschap van kunstmatige intelligentie evolueert snel en een van de opvallende ontwikkelingen is de ontwikkeling van Generative AI. Onder deze, ChatGPT heeft een aanzienlijke impact gemaakt.

Naarmate organisaties deze krachtige tools proberen te integreren in hun workflows, wordt de noodzaak om de toegang tot Generative AI-applicaties te beheersen steeds duidelijker. Voor bedrijven die hun eigen privé ChatGPT-instanties hebben ontwikkeld, is het een kritieke beveiligingsmaatregel om ervoor te zorgen dat dit de enige AI-tool is die toegankelijk is voor hun team, terwijl andere Generative AI-apps worden beperkt.

Gelukkig is er een eenvoudige manier om dit te bereiken met behulp van het Umbrella-dashboard. Dit artikel leidt u door de stappen die u moet nemen om uw organisatie te laten profiteren van uw privé ChatGPT terwijl u strikte controle behoudt over het gebruik van andere AI-toepassingen.

Stap 1: Maak een webregel om uw privéchat-gpt toe te staan

Allereerst moet je inloggen op je Umbrella dashboard. Eenmaal daar, kunt u een DNS-regel of een webregel maken.

Deze regel moet de actie "Toestaan" en een bestemmingslijst hebben met de specifieke URL van uw privé ChatGPT.

Deze stap zorgt ervoor dat gebruikers binnen uw organisatie zonder beperkingen toegang hebben tot uw privé ChatGPT.

Stap 2: Blokkeer alle andere generatieve AI-apps

Onmiddellijk na het maken van de 'Toestaan'-regel moet u een tweede regel maken. Deze regel moet de actie "Blokkeren" hebben en een "Toepassingslijst" bevatten die de categorie Generatieve AI omvat. Door dit te doen, kunt u de toegang tot een breed scala aan populaire Generative AI-applicaties voorkomen, waaronder de openbare versie van ChatGPT.

DNS-beleid

Om ervoor te zorgen dat deze regels effectief worden gehandhaafd bij het gebruik van het DNS-beleid en niet het webbeleid.

Het is van cruciaal belang om de intelligente proxy en SSL-decodering mogelijk te maken voor een naadloze ervaring. Bovendien is de installatie van het Cisco Umbrella root-certificaat noodzakelijk voor de goede werking van de SSL-decodering.

Voor uitgebreide richtlijnen voor het opzetten van het DNS-beleid, kunt u [hier](#) de officiële documentatie raadplegen.

Om de effectiviteit van uw DNS-beleid te optimaliseren, bekijkt u [hier](#) de best practices.

webbeleid

Voor meer informatie over het beheren van webbeleid en het afstemmen ervan op de vereisten van uw organisatie, gaat u [hier](#).

Het implementeren van deze maatregelen stelt uw organisatie in staat om optimaal te profiteren van uw privé ChatGPT en tegelijkertijd het risico op datalekken of afleidingen te beperken die kunnen optreden bij het gebruik van andere Generative AI-apps. De juiste balans tussen veiligheid en toegankelijkheid is essentieel om het potentieel van Generative AI te benutten en tegelijkertijd te zorgen dat de gegevens en bronnen van uw organisatie goed worden beschermd.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.