Intelligenz Welt

GPT-5.5-Cyber

KI-Modellportrait · Quellenstand 2026-10-31



OpenAI/GPT-Anbietericon, kein eigenes Modelllogo · Logo-Quelle / Rechtehinweis. Marken gehören ihren jeweiligen Inhabern. Redaktionelle Identifikation, keine Partnerschaft oder Empfehlung durch den Markeninhaber.

GPT-5.5-Cyber ist eine cyber-permissive Variante von GPT-5.5 von OpenAI für autorisierte Sicherheitsarbeit wie Red Teaming und Penetrationstests, zugänglich nur nach Verifizierung über das Programm Trusted Access for Cyber.

Quellen geprüft am 31. Oktober 2026 · Redaktion: Philipp Paulik

Entwickler: OpenAI →

DAS MODELL EINFACH ERKLÄRT

Mehr Freigabe statt mehr Leistung: das permissive Cyber-Modell richtig einordnen.

GPT-5.5-Cyber ist eine spezialisierte Variante von GPT-5.5 von OpenAI für autorisierte Cybersicherheitsarbeit. Laut OpenAI ist das Modell vor allem permissiver trainiert, nicht leistungsstärker: Es senkt für verifizierte Verteidiger die Ablehnungsgrenze bei Workflows wie Red Teaming, Penetrationstests und kontrollierter Exploit-Validierung. Der Zugang läuft ausschließlich über das Verifizierungsprogramm Trusted Access for Cyber.

Offizielle Dokumentation: GPT-5.5-Cyber

Quellen geprüft: 31.10.2026. Herstellerangaben, kein eigener Modelltest.

Wofür eignet sich GPT-5.5-Cyber?

Für die meisten Sicherheitsteams bleibt laut OpenAI GPT-5.5 mit Trusted Access for Cyber der richtige Einstieg: Secure Code Review, Schwachstellen-Triage, Malware-Analyse, Detection Engineering und Patch-Validierung laufen dort mit präziseren Schutzmaßnahmen. GPT-5.5-Cyber wird erst relevant, wenn autorisierte Workflows trotz TAC an Ablehnungen scheitern - etwa Red Teaming oder Pentests in kontrollierten Umgebungen.

Was GPT-5.5-Cyber von GPT-5.5 unterscheidet

Nach Herstellerangabe ist die erste Vorschau primär permissiver trainiert und soll die Cyber-Fähigkeit von GPT-5.5 nicht signifikant übertreffen; OpenAI erwartet nicht, dass das Modell in jeder Cyber-Evaluierung besser abschneidet. Der Unterschied liegt im Verhalten bei sensiblen, autorisierten Anfragen: weniger klassifikatorbasierte Ablehnungen für geprüfte Verteidiger, kombiniert mit stärkerer Verifizierung, Nutzungsüberwachung und Freigabe-Umfang.

Offizielle Dokumentation: GPT-5.5-Cyber

Zugang über Trusted Access for Cyber

Die Ankündigung beschreibt drei Stufen: GPT-5.5 mit Standard-Schutzmaßnahmen für allgemeine Arbeit, GPT-5.5 mit TAC für die meisten defensiven Workflows und GPT-5.5-Cyber für spezialisierte autorisierte Aufgaben. Einzelpersonen verifizieren sich über chatgpt.com/cyber, Unternehmen über ein Enterprise-Formular. Für die permissivsten Modelle verlangt OpenAI ab 1.6.2026 phishing-resistente Kontosicherung (Advanced Account Security) oder eine entsprechende Unternehmensbescheinigung.

Offizielle Dokumentation: GPT-5.5-Cyber

Für wen das Modell gedacht ist

OpenAI nennt Verteidiger kritischer Infrastruktur und autorisierte Spezial-Workflows: Red Teaming, Penetrationstests und kontrollierte Validierung, etwa Exploit-Nachweise für koordinierte Offenlegung. In der Alpha-Phase wurde das Modell laut Anbieter für automatisiertes Red-Teaming kritischer Systeme und die Validierung hochkritischer Schwachstellen eingesetzt; Details soll ein späterer technischer Bericht liefern. Diese Angaben sind Herstellerberichte, keine unabhängigen Tests.

Offizielle Dokumentation: GPT-5.5-Cyber

Kosten und dokumentierte Grenzen

Die offizielle Preisseite führt gpt-5.5-cyber mit 12,50 USD je Million Eingabe-Token, 75 USD je Million Ausgabe-Token und 1,25 USD für zwischengespeicherte Eingabe. Kontextfenster, maximale Ein- und Ausgabe und unterstützte Endpunkte sind für dieses Modell öffentlich nicht dokumentiert; Annahmen aus den Steckbriefen von GPT-5.5 oder GPT-5.6-Cyber sind nicht zulässig.

Offizielle Dokumentation: GPT-5.5-Cyber

Einordnung in die Modellreihe

GPT-5.4-Cyber war laut OpenAI die erste gezielt cyber-permissiv trainierte Variante. GPT-5.5-Cyber folgte im Mai 2026 als limitierte Vorschau. Im aktuellen API-Katalog steht mit GPT-5.6-Cyber bereits ein dokumentierter Nachfolger, für den OpenAI auf das Daybreak-Programm verweist. Wer neu einsteigt, sollte daher beide Stände prüfen: Preis und ID von GPT-5.5-Cyber sind weiter gelistet, die aktive Weiterentwicklung läuft sichtbar auf die neuere Generation zu.

Offizielle Dokumentation: GPT-5.5-Cyber

Was kostet GPT-5.5-Cyber über die API?

Standard-Eingabe

12.5 USD

je 1 Mio. Texttoken · Basisrate

Standard-Ausgabe

75 USD

je 1 Mio. Texttoken · Basisrate

Standard-Texttoken in USD je 1 Mio. Token laut offizieller Preisseite: Eingabe 12,50, Ausgabe 75, Cache-Eingabe 1,25. Die Preise gelten nur mit Freischaltung über Trusted Access for Cyber; ohne Freigabe ist das Modell nicht nutzbar. Keine Abopreise, keine Steuer- oder Gesamtkostenzusage. Preisstand: 31.10.2026.

Preisstand 31.10.2026. Offizielle Dokumentation: GPT-5.5-Cyber

Vor dem Einsatz prüfen

- Modell-ID gpt-5.5-cyber und den Freigabestatus festhalten; ohne TAC-Verifizierung ist kein Zugang möglich.
- Vor dem Antrag prüfen, ob GPT-5.5 mit Trusted Access for Cyber die eigenen Workflows bereits abdeckt - das ist die Herstellerempfehlung für die meisten Fälle.
- Nachfolger GPT-5.6-Cyber und das Daybreak-Programm in die Planung aufnehmen; Preise, Auflagen und Verfügbarkeit der Preview können sich ändern.

Häufige Fragen zu GPT-5.5-Cyber

Was ist GPT-5.5-Cyber?

Eine cyber-permissive Variante von GPT-5.5 von OpenAI für autorisierte Sicherheitsarbeit. Die offizielle Modell-ID lautet gpt-5.5-cyber; die Bereitstellung erfolgt als limitierte Vorschau über das Verifizierungsprogramm Trusted Access for Cyber.

Wer bekommt Zugang zu GPT-5.5-Cyber?

Geprüfte Verteidiger: Einzelpersonen verifizieren ihre Identität über chatgpt.com/cyber, Unternehmen beantragen den Zugang über ein Enterprise-Formular. Für die permissivste Stufe verlangt OpenAI zusätzlich phishing-resistente Kontosicherung.

Was kostet GPT-5.5-Cyber?

Laut offizieller Preisseite 12,50 USD je Million Eingabe-Token, 75 USD je Million Ausgabe-Token und 1,25 USD je Million zwischengespeicherter Eingabe-Token. Stand: 31.10.2026. Nutzbar ist das Modell nur mit gültiger Freischaltung.

Ist GPT-5.5-Cyber leistungsstärker als GPT-5.5?

Nach Herstellerangabe nein: Die Vorschau ist primär permissiver trainiert und soll GPT-5.5 nicht in jeder Cyber-Evaluierung übertreffen. Für die meisten defensiven Workflows empfiehlt OpenAI weiterhin GPT-5.5 mit Trusted Access for Cyber.

Gibt es GPT-5.5-Cyber als offene Gewichte?

In den geprüften offiziellen Quellen ist nur ein gehosteter, freigabepflichtiger API-Zugang dokumentiert. Eine offene Gewichtslizenz wird nicht genannt.

Alle Antworten beziehen sich auf die verlinkte Herstellerdokumentation und den angegebenen Stand. Kein unabhängiger Benchmark, keine Garantie für Verfügbarkeit oder Ergebnisqualität.

Quellen & Stand

1. OpenAI: Scaling Trusted Access for Cyber with GPT-5.5 and GPT-5.5-Cyber
   Geprüft: 2026-10-31
2. OpenAI: API-Preise, Abschnitt Cyber-Modelle
   Geprüft: 2026-10-31
3. OpenAI: Trusted access for the next era of cyber defense
   Geprüft: 2026-10-31
4. OpenAI: GPT-5.6 Cyber API-Modell
   Geprüft: 2026-10-31
5. GPT-5.5-Cyber: offizielle Ankündigung und TAC-Einordnung
   Geprüft: 2026-10-31

Redaktionelle Zusammenfassung mit KI-Unterstützung, verantwortet von Philipp Paulik. Kein eigener Leistungstest. Änderbare Anbieterangaben gelten für den angegebenen Quellenstand.

Intelligenz Welt · Redaktion: Philipp Paulik · Quellenstand: 2026-10-31
Vollständiges Webportrait: https://intelligenz-welt.de/ki-modelle/gpt-5-5-cyber/
Statischer Export, kein Live-Datenblatt. Preise, Zugriff und Anbieterangaben können sich ändern. Quellen und ihre jeweiligen Abrufstände stehen oben. Impressum · Transparenz