Okta Governance Analyzer

Model Card

Okta Model Cards are intended to provide information about models leveraged by Okta in Okta's product offerings and include information on the intended use cases, limitations, training, and evaluation of models. Model cards are not intended to be technical reports and are provided for informational purposes only. Model cards may be updated from time-to-time.

Model Card: Okta Governance Analyzer

Overview

- **Product/Feature Name:** Okta Governance Analyzer
- **Description:** The model provides recommendations and context to administrative users of Okta Identity Governance to help them make better-informed decisions about when to revoke end user access. Recommendations are generated automatically, not based on specific user queries or inputs. Administrative users see the recommended actions in the user interface and can choose to act on them.
- **Primary Function:** Analysis & Insights: Provides predictions, scores, or analytical insights from data.

Model Details

- **Model Type**: ML (Machine Learning)
- **Model Origin**: In-house developed.
- **Model Provider**: Okta
- **Model Version**: v.1.0
- **Model Architecture**: Binary classification model.

Intended Use & Limitations

- **Intended Use Cases:** It can be challenging for administrative users of Okta Identity Governance (OIG) to determine whether to revoke or modify end user access to various resources. The model is designed to provide recommendations and context for these administrative users to help them make faster and better-informed decisions. The model's recommendations are displayed in the user interface and intended for use by administrative users within OIG.
- **Out-of-Scope Use Cases:** The model is not designed for tasks or scenarios outside of Okta Identity Governance (OIG).
- **Known Limitations:** The accuracy and scope of recommendations are bounded based on the limited scope of data sets consumed by the model.
- **Potential Risks:** What are the potential risks or ways the model could fail or produce problematic outputs? Check all that apply and briefly explain:

Factual Incorrectness (Hallucinations): The model may generate information that is not factually correct.
Bias: The model may produce outputs that are biased against certain demographic groups or reflect societal stereotypes.
Harmful or Inappropriate Content: The model could generate offensive, unsafe, or otherwise inappropriate content.
Other: The recommended actions may not always be correct for the given scenario. The model has been tuned to over-index on "conservative" recommendations (i.e. making recommendations which err on the side of revocation or of least privilege).

Data and Privacy

- **Model Inputs:** Inputs are usage data elements related to various resource access and use attributes.
- **Model Outputs**: The outputs are textual recommendations. For instance, an output recommendation may be "Recommendation: Revoke."
- **Data Minimization**: The model processes discrete usage data elements to provide context and recommendations.
- **Training Data**: The model was trained on usage data from Okta Identity Governance.
- **Is the model trained on Customer Data** (as defined in Okta's Master Subscription Agreement at https://www.okta.com/legal)**?** The model is not trained on Customer Data.

Evaluation and Security

- **Methodology:** The performance of the model is continuously evaluated and the model is subject to continuous monitoring and tuning by Okta.
- **Performance Metrics:** Performance monitoring will be based on defined technical metrics such as F1, precision, and recall scores.

Artificial Intelligence (AI) Principles

Okta strives to safely use and develop AI to strengthen the connections between people, technology, and our community. When it comes to AI innovation, we aim to live our core values and harness the power of AI in a way that reflects said values. This kind of thinking is part of our DNA. That's why we take a values-based approach to AI. Okta's Responsible AI principles underscore (i) transparency; (ii) building customer trust through security, privacy, and safety; (iii) accountability; and (iv) innovating responsibly regarding inclusivity, fairness, and ethics. These principles are aligned with Okta's values: "Love our customers." "Always secure. Always on." "Build and own it." "Drive what's next."

Our developers adhere to responsible AI principles regarding privacy, security, responsible innovation, and more general principles and obligations regarding Customer Data. For more information, please see the published full version of Okta's Responsible AI Principles on Okta.com.

Security and Privacy

- Okta adheres to its existing commitments regarding security, privacy, and confidentiality in connection with Okta products and features that leverage AI that are offered as part of the Okta services.
- Okta follows industry standard processes for testing, developing, and making available products and features that leverage AI for customers.
- Okta has policies and programs in place regarding the use of and governance over AI.
- The data validation measures Okta takes for products and features that leverage AI may vary by product and feature and may include measures like input sanitization, having an allow list of characters that can be passed in the input, having a block list of terms that will be rejected, and having a custom post processing step that validates the output depending on the use case.
- The measures Okta has in place to help ensure that the models leveraged by Okta in Okta's product offerings are accurate and unbiased may vary by product and feature and may include monitoring the performance of models, auditing data to identify inaccuracies or missing information, having a diverse team of developers and data scientists that develop, maintain and improve Okta's products that leverage AI, and having a human in the loop when necessary.

Last Updated Feb 12, 2026