1 Hypothesis

Our hypothesis is that since an SSL model doesn't use any label information the representation learned by such a model will be less susceptible to noisy labeling and ambiguous samples. In contrast a supervised model that uses labels is affected by these factors and the boundary learned by the model is unnecessarily distorted and less smooth which in turn could contribute to more adversarial vulnerability.