The Robot Operating System (ROS) is a popular open-source platform for advanced robotics. Its flexibility and ease-of-use make it well-suited to a wide array of robotics applications; however, these robots are not always sufficiently protected against security threats.

Opportunistic attacks are by far the most prevalent, and robots with inadequate ROS security make tempting targets for bad actors. With that in mind, approaching robotics security proactively is crucial to preventing breaches and saving resources in the long run. Security starts with the underlying operating system, and building robots on Ubuntu unlocks a number of easy, yet effective, measures for maximising protection against the most dominant threats.

Choosing the right OpenStack distribution is essential to the success of an OpenStack project at every organisation. When selecting one, organisations should always follow certain criteria. Is it possible to operate the considered OpenStack distributions economically? How easy is it to deploy them? Can the organisation upgrade its production OpenStack cloud without affecting the workloads? Everyone planning to deploy OpenStack should ask themselves these questions. And there is always more criteria to consider.

In order to facilitate the OpenStack vendor selection process for the organisations, we have recently published an OpenStack distributions comparison website. It highlights the key differences between three leading OpenStack platforms: Canonical’s Charmed OpenStack, Red Hat OpenStack Platform and Mirantis Cloud Platform. Now, in the following blog, I am going to describe some tips which organisations should follow to make sure that they choose...
the right OpenStack distribution.

- **Accelerate AI/ML workloads with Kubeflow and System Architecture** [4]

  AI/ML model training is becoming more time consuming due to the increase in data needed to achieve higher accuracy levels. This is compounded by growing business expectations to frequently re-train and tune models as new data is available.

  The two combined is resulting in heavier compute demands for AI/ML applications. This trend is set to continue and is leading data center companies to prepare for greater compute and memory-intensive loads for AI.

- **FIPS 140-2: Stay compliant and secure with Canonical** [5]

  FIPS 140-2 is a set of publicly announced cryptographic standards developed by the National Institute of Standards and Technology. It is an essential part of FEDRamp requirements for many governmental agencies in the US and Canada, as well as their business partners from all around the world. Furthermore, as a well established and verified security standard, an increasing number of large companies and financial institutions are asking for FIPS compliance.

  Yet, FIPS certification process introduces challenges that could impact your security. Ubuntu lets you choose the way to implement FIPS-certified cryptographic modules with two distinct FIPS alternatives to choose from to overcome those challenges.

**Ubuntu**

**Source URL:** [http://www.tuxmachines.org/node/135888](http://www.tuxmachines.org/node/135888)

**Links:**
[1] [http://www.tuxmachines.org/taxonomy/term/121](http://www.tuxmachines.org/taxonomy/term/121)
[3] [https://ubuntu.com/blog/openstack-distributions](https://ubuntu.com/blog/openstack-distributions)