ubuntu

CANONICAL

Cybersecurity with Ubuntu

Ubuntu, a platform that improves your IT productivity, enables your cybersecurity strategy while keeping your budget under control

Keeping an organization safe and implementing a robust cybersecurity framework is a task beyond a particular software or solution. Enterprises need a reliable operating system to power the organization's workloads on the public or the private cloud while it enables their cybersecurity strategy as well as their industry sector or national requirements.

With Ubuntu Advantage, the enterprise-grade subscription for Ubuntu, customers leverage an operating system designed with the security mindset for today's security landscape but also get a trusted partner of the open source community that enables open source applications for high security and regulated environments, such as FIPS 140 and Common Criteria while it collaborates with security organizations to gain access to vulnerabilities before they are public. Ubuntu Advantage sets the foundation for a cybersecurity framework, with provenance, vulnerability management, hardening and compliance profiles such as CIS and DISA-STIG, while offering competitive economics.

Key benefits

Predictable lifecycle

Ubuntu LTS releases are made available every two years and are maintained for ten years with Ubuntu Advantage. Each release comes in two five-year phases, Standard support and Extended Security Maintenance, both including security updates and kernel livepatching.

<table>
<tr><th colspan="10">Ubuntu LTS release</th></tr>
<tr><td colspan="5">Standard Support phase</td><td colspan="5">Extended Security Maintenance phase</td></tr>
<tr><td colspan="5">Maintenance updates</td><td colspan="5" rowspan="2">Security updates</td></tr>
<tr><td colspan="5">Security updates</td></tr>
<tr><td colspan="5">Livepatching</td><td colspan="5">Livepatching</td></tr>
<tr><td>Yr1</td><td>Yr2</td><td>Yr3</td><td>Yr4</td><td>Yr5</td><td>Yr6</td><td>Yr7</td><td>Yr8</td><td>Yr9</td><td>Yr10</td></tr>
</table>

Available with subscription
Available free of charge driving our mission

Certified Compliance

Regulated and high security environments have complex requirements as they are designed to tackle many threats, known and unknown. Therefore, developing or running workloads in these environments requires rigid certifications. Ubuntu Advantage provides access to the necessary artifacts to comply with Common Criteria, an international (ISO/IEC 15408) computer security certification for high security environments, and FIPS 140, the U.S. government data protection profile.

Secure configuration & hardening

The default configuration of Ubuntu balances usability and security. However, systems carrying dedicated workloads can be further hardened to reduce their attack surface. Canonical works with DISA to ensure the Security Technical Implementation Guides (STIG) are available for Ubuntu, and Ubuntu Advantage customers get access to certified CIS benchmark content to harden with the widely accepted hardening guide using the OpenSCAP tooling.

Vulnerability Management

System administrators are constantly being challenged from attackers looking for access in their infrastructure by exploiting software vulnerabilities. Defending infrastructure requires timely access to software security updates, security advisories, machine readable OVAL data for SIEM integration and automation, including kernel livepatching, for the lifecycle of the systems. Extended Security Maintenance (ESM), ensures that all the above are provided for Ubuntu's 10-year lifecycle. Furthermore, Canonical ensures timely fixes in vulnerabilities on the operating system, and targets a response time of up to 1 day on average for critical and up to 14 days on average for high severity vulnerabilities.

Anti-exploitation defenses

Malicious software (malware) is the primary threat to organisations today, and can have a severe impact on operations. Using malware, attackers might be able to capture passwords, steal or even destroy sensitive corporate data. Ubuntu comes with state of the art anti-exploitation malware defenses. It enables the latest industry best practices against vulnerability exploitation vectors, such as heap and stack protections, Address Space Layout Randomization (ASLR), non-executable memory, and applications are compiled to take advantage of the latest CPU security features such as Intel's Control-Flow Enforcement Technology (CET). Ubuntu systems support UEFI secure boot, and receive automatic security updates by default.

How does Ubuntu Advantage compare to RHEL and SLES?

While all companies distribute an operating system based on Linux, the technical implementations are very different. Ubuntu is based on the community-led Debian operating system, deriving conventions from it, while RHEL derives from Fedora (community based but led by Red Hat) and SuSe from OpenSuSe. The commercial terms are also very different with Ubuntu Advantage having a simple per host and per VM pricing policy.

1. Physical systems can host unlimited VMs

Get started with Ubuntu

To purchase Ubuntu Advantage, including the cybersecurity offering please visit ubuntu.com/advantage or contact our team below.

(UK) +44 203 656 5291
(US) +1 737 2040291
email: sales@canonical.com

CANONICAL