

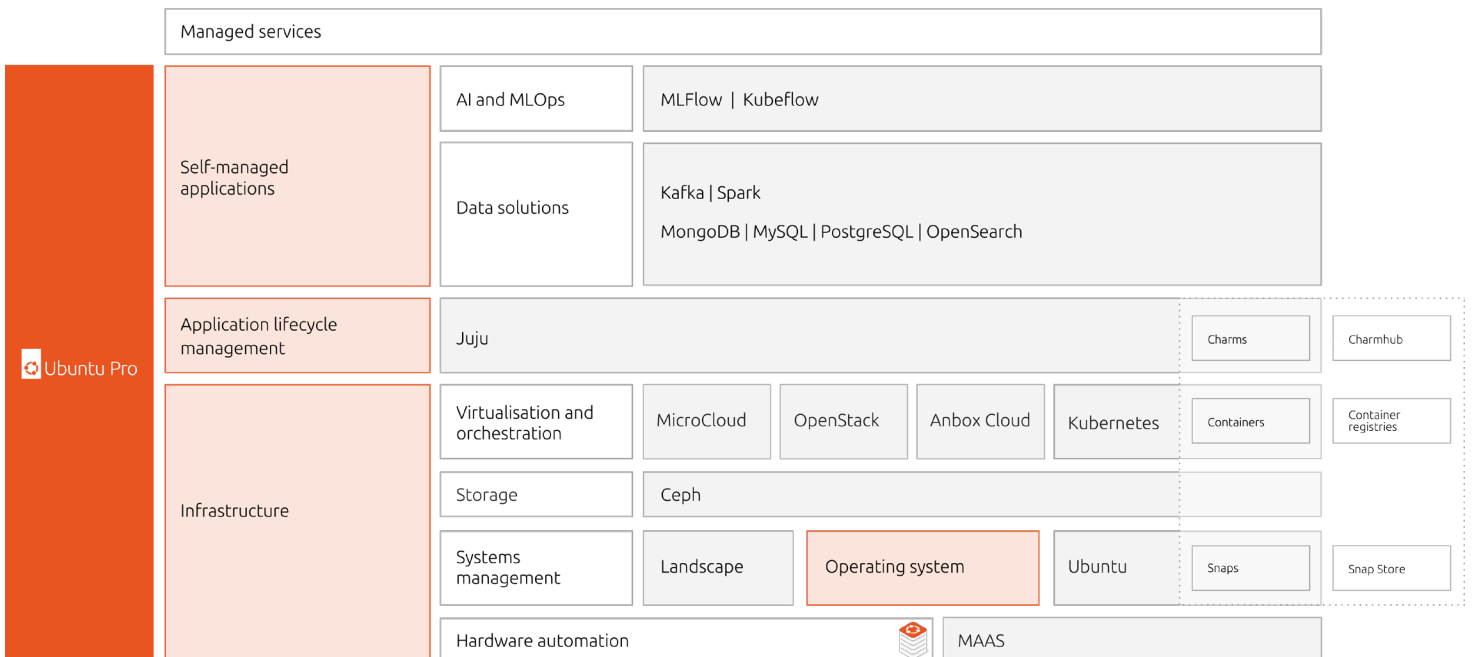
Secure your enterprise software supply chain

Let your developers focus on value-added work. Let us handle the security patching. Access powerful patching automation and estate management tools to ensure compliance.



Up to 15 years of security maintenance

Research tells us that 7 in 10 teams spend almost a full day per week applying patches (IDC, 2025). That's a full day they could be spending on building new features. With Canonical's Ubuntu Pro subscription, your team can focus on your business while open source experts handle security maintenance for your open source software and its dependencies. We do this for up to 15 years in line with the maintenance period of every Ubuntu LTS release, testing and backporting security fixes to provide stability for your environment.



Reliable security coverage for open source software

Over the network runtime dependencies



Compile-time dependencies



Local runtime dependencies



Operating system

Ubuntu Pro provides reliable security maintenance for your open source components, offering consistent support across a variety of packaging formats at every layer of your operations. This includes timely patches for critical vulnerabilities.

Examples include Postgres, Valkey, MySQL

Examples include Python packages

Examples include OpenJRE, glibc

Ubuntu OS

We help your team secure all layers of its open source dependencies

OUR SECURITY COVERAGE EXTENDS TO:

Debian packages (debs)

Ensuring the security of open source packages in Ubuntu's Main and Universe repositories.

Containers

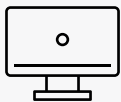
Security maintenance for [container images built by Canonical](#) and their content, through our Container Build Service.

Charms

Delivering security updates for software operators in our portfolio.

UBUNTU PRO IS AVAILABLE ON:

Desktops



Servers



Public clouds



IoT devices



AUTOMATE PATCHES, MANAGE AND MONITOR YOUR ESTATE

Automate installation, security patching, auditing, access management and compliance tasks for thousands of remote, edge, virtual, or physical devices. Canonical's Landscape makes it simpler to manage the most complex fleets of up to thousands of machines in connected or air-gapped environments, all through a single portal.



Comprehensive systems management

Get a unified platform for managing large-scale Ubuntu deployments, simplifying operations, automating hardening, and applying security patching – creating a faster pathway to regulatory compliance.

Flexible deployment options

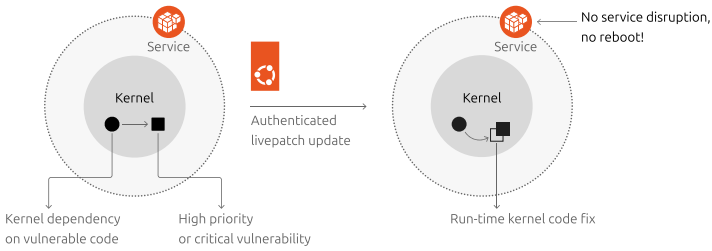
Deploy and update in any network environment, including air-gapped or limited network setups.

Extensible integration

Integrate our powerful estate management easily into your existing IAM, SSO, and monitoring systems – with greater customization options via our API.

[Learn more about Landscape](#)

PATCH CRITICAL AND HIGH VULNERABILITIES IN THE KERNEL WHILE AVOIDING DOWNTIME



Shrink your exploit window for critical and high severity Linux kernel vulnerabilities, by patching the Linux kernel between security maintenance windows while the system runs. Livepatch can be consumed as a SaaS service or deployed on-prem in air-gapped environments.

Added security without downtime: defer reboots to the next maintenance window

Smaller exploit windows: secures the Linux kernel against critical and high vulnerabilities between scheduled maintenance windows

Over a decade of security patches: get patches for the General Availability (GA) kernel and the latest Hardware Enablement (HWE) kernel for an Ubuntu LTS release

Granular control over patch rollout: ensures system administrators can set incremental roll-outs or tiered patch rollouts

Safety-first architecture: Livepatch operates in a sandboxed environment, built-in backup mechanisms, and automatic rollback capabilities

Enabled in just one command: deploy with a simple `$ pro enable livepatch`

CASE STUDY

[Read the full case study >](#)

GMO Pepabo goes from 2,500 hours of manual migrations and patching to just 32 hours with Livepatch



Livepatch is included with Ubuntu Pro.
[Learn more about Livepatch](#)

Hardening and support mandatory compliance

There are countless security standards and regulations that you are required to meet. Ubuntu Pro provides much of what you need to help you meet the most stringent security standards, including hardening profiles and security configurations. The Ubuntu Security Guide simplifies compliance for major global cybersecurity regulations and legal requirements, significantly cutting costs compared to manual processes.

MEET COMPLIANCE REQUIREMENTS FOR:

FIPS
CMMC
FedRAMP
NIS2
DISA-STIG

The EU Cyber Resilience Act
NIST 800-53
UK Cyber Essentials
CIS
PCI-DSS
HIPAA

CASE STUDY

[Read the case study >](#)

Ubuntu Pro helps a service provider reach FIPS compliance and generate CIS benchmarks – easy and fast



GET COMPREHENSIVE SECURITY COVERAGE AND FAST TRACK COMPLIANCE

Start your 30-day free trial of Ubuntu Pro today, and experience enterprise-grade security and compliance. Ubuntu Pro is free for personal use and on up to 5 machines.

[Explore Ubuntu Pro's value](#)

[Try for free for 30 days](#)

[Learn more about how Canonical secures your software supply chain](#)