Canonical

Maximising security and compliance in the US public sector with Ubuntu Pro



Executive summary

Within the US Public Sector there are many security and compliance requirements amongst many other regulations. Finding your way through all the rules and recommendations is complicated and time-consuming. Yet, this is nothing compared to actually sourcing and deploying a technology solution that is easy to use, has enterprise-grade security, is cost-effective, whilst also meeting all these compliance requirements. The operating system is the foundation of your technology stack, and likely one of the first enablers you will need to carefully select to deliver on your compliance strategy.

It's likely that IT staff within your organisation already use Ubuntu, as it is the most popular Linux distribution for developers and the most widely deployed operating system in the cloud. Canonical, the publisher of Ubuntu, has put a lot of thought into developing a set of features and capabilities that allow you to deploy it easily in a secure and compliant manner for public sector use cases. This guide will cover the intricate compliance landscape faced by organisations working in the public sector and how Ubuntu Pro can be used to meet the industry's strict security standards and requirements.

Contents

Executive summary 2

Public sector security and compliance landscape 4
- FIPS 140 4
- DISA STIG 4
- CIS benchmarks 5
- FedRAMP 5

Solving compliance complexity with Ubuntu Pro 6
- FIPS 140 Cryptography 6
  - Strict versus Updates 7
  - Using the Security Policy 8
  - FIPS 140-2 versus 140-3 8
- DISA STIG and CIS compliance automation with Ubuntu Security Guide 8
  - Automated hardening with the Ubuntu Security Guide 9
  - Manual hardening steps 10
- 10-year security maintenance with Ubuntu Pro for FedRAMP 10
  - Main or Universe packages 10
  - Applying the updates 11
  - Ubuntu Security Notices and OVAL data 11
  - Avoiding downtime with Kernel Livepatch 12
- Controlled access management with Active Directory integration 12
- System administration with Landscape 13
- Using Ubuntu in air-gapped environments 14
- Compliance automation in public clouds 15
  - AWS GovCloud 15
  - Azure Government 16

Ubuntu Pro: all-in-one security and compliance 16

Further reading 17

Public sector security and compliance landscape

A complex set of standards and regulations govern compliance for organisations in the US public sector and their vendors. This section provides an overview of these requirements.

FIPS 140

FIPS 140 is a US and Canadian government data protection standard that defines the design, configuration and deployment of cryptographic modules. A data protection standard dedicated to cryptography is necessary because of the vital role that cryptography plays in the modern technology landscape, underpinning the security of the internet. Implementing cryptography correctly is notoriously difficult, as the slightest mistake or weakness quickly undermines the whole security model of the applications and data that build on top of it.

US Federal agencies and anyone deploying systems and cloud services for Federal government agency use, whether directly or through contractors, are required to run workloads with FIPS 140 validated cryptography. FIPS 140 has also been adopted outside of the public sector in industries where data security is heavily regulated, such as financial services (PCI-DSS) and healthcare (HIPAA). It is a mandatory requirement for government departments that collect or handle sensitive data.

The standard defines which algorithms can be used, based on the latest industry knowledge and academic research, and how to deploy them securely. Each cryptographic module is thoroughly tested and validated against the standard by an independent NIST-accredited testing laboratory to ensure that the implementation is robust and fit for use.

FIPS 140 is required under multiple compliance regimes, such as the Federal Risk and Authorization Management Program (FedRAMP), the Federal Information Security Management Act of 2002 (FISMA) and the Health Information Technology for Economic and Clinical Health Act (HITECH).

DISA STIG

Security Technical Implementation Guides (STIG) are developed by the Defense Information System Agency (DISA) for the US Department of Defense. A STIG is a configuration standard consisting of guidelines for hardening a system to decrease its exposure and make it more difficult to hack. System hardening means reducing the attack surface: removing unnecessary software packages, locking down default values to the tightest possible settings and configuring the system to only run what you explicitly require. System hardening guidelines also seek to lessen the potential collateral damage in the event of a compromise.

Any computer or system that connects to a Department of Defense (DoD) network is required to be hardened in accordance with the relevant STIG. The STIGs have also been adopted more broadly across the public sector, including the latest revision of the NIST SP 800-53 (Security and Privacy Controls for Information Systems and Organizations) which applies to any organisation handling classified information.

STIGs are intended to be guides: if a specific rule cannot be matched exactly this is not necessarily a concern as long as the intention of the security requirement backing the rule can be met by some other means.

STIGs are divided into three categories, relating to their security impact.

- **CAT I:** Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Availability, or Integrity

- **CAT II:** Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity

- **CAT III:** Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity

Administrators will want to ensure that they have no outstanding Cat I issues, and ideally no Cat II issues either.

CIS benchmarks

Similar to DISA STIGs, the CIS benchmarks are widely adopted system hardening guides that are applicable to almost every modern production environment. They are published by the Center for Internet Security, an independent body which maintains hardening standards for all major operating systems and applications. CIS works with both the software vendors and the wider security community to generate industry standard guidelines incorporating the latest security research and threat intelligence.

FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is a US federal government-wide security and compliance program for cloud service providers. In order for federal agencies to use cloud services, the provider must be FedRAMP authorised. The security controls within FedRAMP are based on the NIST SP 800-53 standard.

There are three impact levels defined for RedRAMP: low, medium and high. The three levels have more stringent security controls at each stage.

1. Low impact is aimed at services for which a security incident would only have a limited negative effect on an agency's mission.

2. Moderate impact covers the majority of service providers and is aimed at services where a security incident would have a serious impact on the agency.

3. High impact is geared towards emergency services, law enforcement, and other critical systems where a security breach would be catastrophic.

Many of the FedRAMP security controls are aimed at the operating procedures of the organisation, and one of the key components is access control: managing user accounts, access rights and privileges. Most organisations use Active Directory to implement their identity and access management policies.

The standard includes several areas which specifically target the technology deployment. FIPS 140 cryptographic modules must be used. Systems must be hardened according to recognised hardening standards, such as the CIS benchmarks or DISA STIG, and security vulnerabilities must be patched within a defined timeframe.

We'll now cover the enterprise-grade features available with Ubuntu Pro that help organisations meet these different compliance requirements.



Solving compliance complexity with Ubuntu Pro

Ubuntu Pro is Canonical's subscription for enterprise-grade security, support and compliance. This section details how organisations can make use of Ubuntu Pro's features to comply with different public sector standards and implement compliance and security measures at scale.

FIPS 140 Cryptography

Canonical provides FIPS 140 certified cryptographic modules that are a direct drop-in replacement for the standard cryptography libraries which ship with Ubuntu by default. By installing these components, the system libraries provide a means for applications to use cryptographic algorithms and protocols in accordance with the requirements of the FIPS 140 standards.

These crypto modules are made available for all Ubuntu LTS (Long Term Support) versions, which are released every two years in April. The NIST certification process to validate the modules takes many months and so the FIPS modules will not be available immediately at release time, but released once NIST has completed the certification.

FIPS modules have been provided for all LTS releases since Ubuntu 16.04, and include the following libraries and components:

- Linux kernel
- OpenSSL
- OpenSSH
- Libgcrypt
- StrongSwan

For OpenSSH, since Ubuntu 20.04 LTS the key derivation cryptography functionality has been updated to use the OpenSSL library, meaning that the OpenSSH package itself does not need to be separately certified for FIPS 140 compliance.

Strict versus Updates

An important decision needs to be made when considering how to consume these FIPS components. The NIST certificates are strictly valid for one binary version of the module, running on the exact same hardware configuration. As mentioned earlier, the time to certification can take months, or in some cases more than a year, and the consequence of this is that there will frequently be security vulnerabilities discovered during this time. Canonical patches security vulnerabilities in all supported packages as part of its famous 10-year security maintenance guarantee, but the certified modules will miss out on these patches in order to be strictly compliant with the NIST certificates. To address this obvious security shortcoming, Canonical provides patched crypto modules which we term “fips-updates”. These are not the exact binary versions of the certified components, but do include the all-important vulnerability fixes, and we strongly recommend that everyone uses these security-updated modules unless they have a compelling reason not to do so.

In order to install these modules, you need to have an Ubuntu Pro subscription; they are made available through the Ubuntu Pro client. The Pro client gives the option to choose either the “fips” or “fips-updates” entitlement - and we suggest choosing “fips-updates” in almost all cases. Once this is enabled, the client downloads the FIPS versions of the packages and replaces them over the defaults.

```
$ sudo pro status
SERVICE              ENTITLED  STATUS      DESCRIPTION
esm-apps             yes       enabled     Expanded Security Maintenance
for Applications
esm-infra            yes       enabled     Expanded Security Maintenance
for Infrastructure
fips                 yes       disabled    NIST-certified core packages
fips-updates         yes       disabled    NIST-certified core packages
with priority security updates
livepatch            yes       enabled     Canonical Livepatch service
usg                  yes       disabled    Security compliance and audit
tools

Enable services with: pro enable <service>


$ sudo pro enable fips-updates
One moment, checking your subscription first
This will install the FIPS packages including security updates.
Warning: This action can take some time and cannot be undone.
Are you sure? (y/N) y
Updating package lists
Installing FIPS Updates packages
FIPS Updates enabled
A reboot is required to complete install.
```

In order to check whether an Ubuntu system has FIPS enabled, you can check the flag that the kernel sets:

```
cat /proc/sys/crypto/fips_enabled
1
```

Using the Security Policy

Canonical supplies a Security Policy alongside the NIST certificate, and this is a useful document that serves two main purposes. The first part lists the rules under which the modules must operate in order to comply with the regulations. The second part is the description of how our modules meet the requirements with specific reference to the publication. The Security Policy is a good resource to start using when designing your application for FIPS, or adapting an existing application to fit in with the requirements.

Will your application be automatically compliant with regulations, provided the Ubuntu host system has FIPS enabled? This is a frequently asked question. In short, the answer is no: you need to ensure that any cryptographic operation that your application is doing makes use of the appropriate module in accordance with the published Security Policy document. For example, if you have a C++ application, you can't just use a library such as crypto++ as this has not been validated - you need to use OpenSSL in accordance with its Security Policy.

FIPS 140-2 versus 140-3

The FIPS 140-2 standard was first published in 2001, and a lot has changed in the world of cryptography since then. NIST published a brand new standard, 140-3, in September 2019, to replace the venerable 140-2. Since 2022, new modules can only be certified against the new standard, although existing certificates for 140-2 do remain valid until their sunset date, or 2026 at the very latest.

When it comes to a requirement for FIPS-validated cryptography, either 140-2 or 140-3 modules will be suitable for use, as long as they are still within their 5-year certification period. For Ubuntu specifically, the Ubuntu 18.04 LTS modules remain valid until 2025, and the 20.04 LTS modules until 2026 - both of these releases are 140-2. From Ubuntu 22.04 onwards, all modules will be certified for 140-3.

DISA STIG and CIS compliance automation with Ubuntu Security Guide

Vendors like Canonical produce specific rules that apply DISA-STIG requirements to their product, subject to approval by DISA. STIGs are produced for physical devices such as firewalls, software applications such as Microsoft Active Directory, and for operating systems including Ubuntu.

What does hardening an operating system like Ubuntu mean? The STIGs include many rules to lock down settings and configuration options. These settings aim to limit the ability for low-privileged users to gain access to shared resources. They reduce the potential exposure of a system breach, and enforce strict auditing of all user actions that could impact the security of the system. For operating systems, the STIG includes a strict requirement for FIPS-validated cryptographic modules.

DISA's list of available STIGs is available and searchable through a Document Library. This list includes the new versions of the STIGs that are published regularly.

CIS benchmarks are also available for all Long Term Support Ubuntu releases since 16.04. These benchmarks come in several different versions: levels 1 and 2, for both servers and for workstations. Level 1 is designed to "be practical and prudent; provide a clear security benefit; and not inhibit the utility of the technology beyond acceptable means". Level 2 goes a step further, is "intended for environments or use cases where security is paramount; acts as defence in depth measure; and may negatively inhibit the utility or performance of the technology". The server benchmarks are intended for situations where there is no GUI, while the desktop version takes the normal GUI environment into consideration.

Automated hardening with the Ubuntu Security Guide

The STIG or CIS benchmarks for an operating system such as Ubuntu can include over 300 individual rules to check and remediate if necessary. This can be an overwhelming prospect, so in order to simplify the process Canonical publishes the Ubuntu Security Guide (USG), an automation tool that handles the checking and remediation of the STIG rules.

USG is available as part of Ubuntu Pro, and can be enabled through the Pro client:

```
$ sudo pro enable usg && sudo apt install usg
One moment, checking your subscription first
Updating package lists
Ubuntu Security Guide enabled
Visit https://ubuntu.com/security/certifications/docs/usg for the next steps
```

USG comes with several in-built profiles: CIS benchmarks with versions for desktop and server, and the DISA-STIG.

Running USG to bring a system into compliance with the benchmark is straightforward:

```
$ sudo usg fix disa_stig
```

Having run the fix command, and rebooted to ensure that all the changes have been picked up, the next step is to audit the system and determine which of the STIG rules have been satisfied and which are outstanding.

Run this command to perform an audit of the updated system:

```
$ sudo usg audit disa_stig
```

The audit command produces an HTML output document that details the findings along with their severity.

Manual hardening steps

There are some rules within the STIG that cannot be easily automated by USG, and should be applied manually to attain full coverage:

- **McAfee Endpoint Security Software** - this is a piece of third-party software that needs to be acquired and installed.
- **Encrypted disk partitions** - these need to be prepared at installation time, and can't be easily retrofitted to existing non-encrypted partitions.
- **Offload audit logs to external media** - this needs to be set up manually.
- **Set the UEFI boot loader password** - this should be set with a user-supplied password.
- **Hardware Tokens for Authentication** - multi-factor hardware tokens should be deployed by the system administrator.

10-year security maintenance with Ubuntu Pro for FedRAMP

Configuring your system to be compliant with FIPS and similar standards is one step in the security and compliance journey. But security vulnerabilities are a fact of modern life and ensuring you apply timely patches to remediate any vulnerabilities is equally important.

Even outside of FedRAMP specifically, any organisation running production workloads will be concerned with keeping their software and applications up-to-date with the latest security fixes. In Verizon's 2022 Data Breach Investigation Report, it was found that only 25% of the scanned organisations patched known vulnerabilities within two months of their public disclosure, demonstrating the crucial importance of applying security fixes as soon as they become available. Canonical typically patches critical vulnerabilities within 24 hours of their disclosure, and this wide discrepancy highlights one of the biggest challenges facing engineering teams today: managing security vulnerabilities in a timely manner.

A default install of Ubuntu LTS comes with five years of security updates for the Main packages in the distribution. Ubuntu Pro provides security fixes for the entire distribution (Main and Universe packages) for ten years, with extensions for industrial use cases.

Main or Universe packages

The pro command-line tool enables you to determine how many packages are installed from the Main or Universe repositories:

```
$ pro security-status
925 packages installed:
   880 packages from Ubuntu Main/Restricted repository
   45 packages from Ubuntu Universe/Multiverse repository

To get more information about the packages, run
   pro security-status --help
for a list of available options.

This machine is receiving security patching for Ubuntu Main/Restricted
repository until 2027.
This machine is NOT attached to an Ubuntu Pro subscription.

Ubuntu Pro with ‘esm-infra’ enabled provides security updates for
Main/Restricted packages until 2032.

Ubuntu Pro with ‘esm-apps’ enabled provides security updates for
Universe/Multiverse packages until 2032 and has 1 pending security update.

Try Ubuntu Pro with a free personal subscription on up to 5 machines.
Learn more at https://ubuntu.com/pro
```

This example shows a mixture of packages from the Main and Universe repositories, and highlights that there is a security update for an application that is available for Ubuntu Pro subscribers.

Applying the updates

In order to make security patching as seamless and disruption free as possible, Ubuntu includes the capability to install security updates automatically on a daily basis with the unattended-upgrades package.
Updates can also be applied manually. The simplest way is to run apt update and apt upgrade. This pulls in all the latest fixes and updates and ensures that the system will be fully patched against all known vulnerabilities, and this facility is one of the reasons for Ubuntu’s enduring popularity. In cases where individual security fixes need to be applied selectively, they can be deployed with the pro fix command, which takes either the CVE number or the USN (Ubuntu Security Notice) reference as a parameter.

Ubuntu Security Notices and OVAL data

Each time the Canonical security team identifies and fixes a vulnerability, an Ubuntu Security Notice (USN) is published to the website. The USNs provide details of the security issue, which versions are affected, and link to the original CVE report pages.

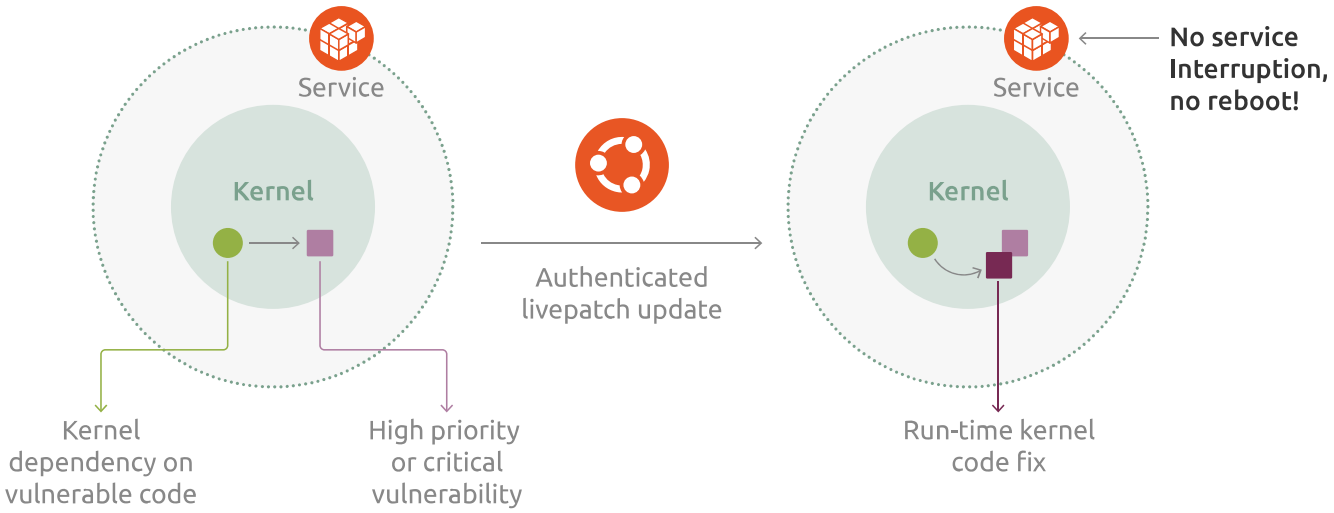
Canonical also produces OVAL data (Open Vulnerability Assessment Language) - an industry standard format for describing vulnerabilities and their status - which can be consumed by a range of third party scanning tools. OVAL data is a machine-readable format that can be used to evaluate and manage security risks related to any existing Ubuntu components. This is a key part of any security compliance program or Information Security Management System, providing the capability to audit systems and applications and generate evidence demonstrating effective patching and on-going security awareness.

Avoiding downtime with Kernel Livepatch

Another reason that security patches might not be applied in a timely manner is when the system needs to be rebooted, for example when fixing vulnerabilities in the Linux kernel. Canonical provides Livepatch as part of Ubuntu Pro, which enables security patches to be applied directly to a running system without requiring an immediate reboot. This is particularly beneficial in FedRAMP environments where critical vulnerabilities must be patched within an enforced time window, and where 5-9s uptime is imperative.

Livepatch is available for Ubuntu LTS release kernels as well as Hardware Enablement (HWE) kernels - this page describes the Ubuntu kernel lifecycle. Livepatch is also only available for x86_64 architectures, although this covers the vast majority of server deployments.

Whilst Livepatch avoids the need for an immediate reboot, systems are still subject to regular maintenance requirements. Maintaining Livepatches becomes incrementally more complex with each security fix that is published, and so Canonical can provide up to nine months of Livepatches for running kernels, but after that time the system will need to be rebooted to reset the nine-month window.



Critical kernel vulnerabilities are patched in real-time by deploying the security patch as a kernel module.

For customers needing to run their estate in an air-gapped environment or behind firewall restrictions, it is also possible to run a local kernel Livepatch server on-premise. Providing the update server can reach Canonical's servers to pull the latest fixes, these can then be applied to air-gapped systems.

Controlled access management with Active Directory integration

FedRAMP and other compliance regimes based around the NIST Cybersecurity Framework have comprehensive Identity and Access Management (IAM) requirements. To implement these requirements, many organisations use Active Directory.

Linux desktops, including Debian and Ubuntu, have supported Active Directory integration for a long time through SSSD; however, that was limited to authentication and a small subset of related security policies. Canonical has released ADsys, an Active Directory client, which allows for:

- Native Group Policy Object support for both machine and user policies targeting dconf settings on the client machine.
- Privilege management, allowing the possibility to grant or revoke superuser privileges for the default local user, and Active Directory users and groups.
- Custom scripts execution, giving the possibility to schedule shell scripts to be executed at startup, shutdown, login and logout.
- Active Directory Administrative Templates for all supported versions of Ubuntu.
- Native user authentication with Azure Active Directory (Azure AD), enabling users on Microsoft 365 (M365) Enterprise plans to authenticate Ubuntu desktops with the same credentials they use for M365 or Azure.

ADSys is supported on Ubuntu starting from 20.04.2 LTS, and is tested with Windows Server 2019. These features align the Active Directory management experience of Ubuntu as closely as possible to the one available in Windows. Many organisations have well-established infrastructure, policies and procedures based on Active Directory, and Ubuntu's AD integration allows administrators to manage Linux systems with the same tools that they are familiar with.

System administration with Landscape

Landscape is the leading management and administration tool for Ubuntu, allowing IT staff to take control of their Linux infrastructure, and improving security at scale. Landscape is available with Ubuntu Pro, and forms an important part of managing and auditing Linux assets within regulated and security-conscious environments.

Landscape enables automation for security, hardening and compliance. By providing a single view-point into the status of the whole estate, Landscape allows administrators to ensure that all security patches have been applied, and enables them to fix any security issues and deploy updates remotely. This overview also extends to hardening and compliance: Landscape enables administrators to scale out the generation of audit reports with the Ubuntu Security Guide to provide evidence of the state of compliance to hardening standards across the fleet. Time-series graphs provide a long-term view of the state of compliance over time, to give assurances that no breaches of security have occurred, and auditing can be customised with categorised event logs to create targeted reports.

For more complex tasks, Landscape includes a comprehensive API allowing a wide range of administrative functions to be carried out at scale across the deployment.

Accurate and effective asset management is a key requirement in security frameworks such as FedRAMP, along with configuration management, and Landscape provides these capabilities for both administrators and auditors.

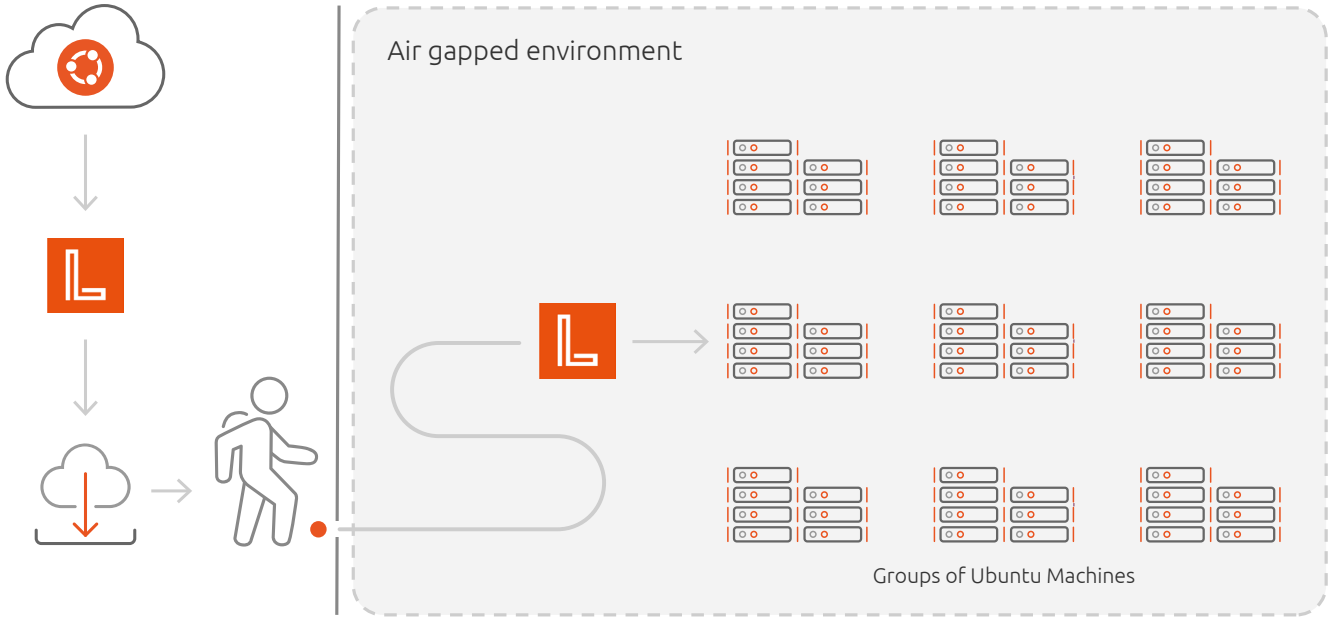
Landscape is available with Ubuntu Pro to deploy on-premise, to consume ready-to-go as a SaaS, and also as a managed service.

Using Ubuntu in air-gapped environments

In order to provide maximum security against external threats, the ultimate defence mechanism for technology deployments is to disconnect the network from the public internet, in what is known as an “air-gapped” scenario. There are variations on this theme, where firewalls can be used to block internet traffic instead of physically unplugging the network devices, but the end result is the same: the controlled environment is completely isolated from the outside world. This mechanism provides excellent security, but at the cost of a much more cumbersome deployment and update procedure.

Security vulnerabilities are discovered on a daily basis, and software vendors such as Canonical issue security patches in a timely manner to prevent customers being at risk of running vulnerable systems. These patches are most typically available over the internet, which means that air-gapped environments can’t receive the fixes directly.

To keep systems up to date with security patches, a proxy of some sort is required. This is most easily accomplished on Ubuntu using Landscape, which includes the capability to make a mirror of the Canonical software repositories.



Landscape deployment in an air gapped environment

The recommended deployment for Landscape in air-gapped environments can be summarised as follows:

1. Install one Landscape server on an internet-connected network
2. Use it to mirror (take a copy of) the Ubuntu software and update repositories
3. Take a physical copy of the mirror and import this into another Landscape server running within the air-gapped network using the Landscape API

The same procedure applies to the Livepatch server, enabling the complete suite of Ubuntu Pro compliance and security features to be deployed and managed in air-gapped environments where this is a requirement.

Air gapped setups provide a high degree of security assurance, but at the cost of increased installation and maintenance time. For workloads with less stringent security requirements, it can be much faster to make use of public clouds instead.



Compliance automation in public clouds

Ubuntu can be deployed even more simply in the public cloud than on-premise. Canonical works with all the major cloud platform providers to ensure that Ubuntu runs flawlessly on their customised hardware, and that the Ubuntu fleet can be managed effectively using the cloud-native tools and dashboards. Integrated billing means that Ubuntu instances can be spun up without needing to on-board a new vendor or go through additional procurement processes.

For the US federal government, several of the public clouds offer dedicated regions specifically for deploying restricted workloads.

AWS GovCloud

AWS GovCloud is a separate AWS region for government agencies and contractors, designed to meet their regulatory and compliance requirements. It is suitable for use with Controlled Unclassified Information, PII, PHI, finance and law-enforcement data, and is logically and physically separated from the rest of the AWS regions.

GovCloud is capable of hosting missions that require FedRAMP High Baseline level, Department of Justice CJIS, ITAR/EAR, DoD Cloud SRG Impact Levels 2,4 and 5, and FIPS 140. It is operated by US citizens on US soil, and is only accessible to US entities and persons.

Ubuntu Pro is the same image in AWS GovCloud and standard AWS regions, and with in-place upgrades available it is possible to convert existing Ubuntu images to Pro with AWS, enabling integrated billing directly with the cloud.

Azure Government

Azure Government is a collection of dedicated Azure regions: US Gov Arizona, US Gov Texas, and US Gov Virginia, that allow federal departments and agencies to deploy their missions in cloud environments that require up to FedRAMP High, ITAR/EAR, DoD SRG Impact Levels 2, 4 & 5, and Level 6 with Azure Government Secret. Azure Government runs in logically and physically separated environments, and is operated by US citizens subject to background screening checks. Ubuntu Pro is available in Azure Government as well as standard Azure regions.

Ubuntu Pro: all-in-one security and compliance

All of the pieces of functionality described above are available with an Ubuntu Pro subscription. Ubuntu Pro helps enterprises and organisations empower their developers to use anything in Ubuntu with confidence, knowing it will be secured for ten years and meet their compliance obligations. In order to make it easy to understand and deploy, one single subscription gives access to all the Pro functionality at once, with no extras or bolt-ons required.

Up-to-date pricing is available at ubuntu.com/pro.

Ubuntu Pro is also available for a no-obligation free trial to enable anyone to test it out and see if it fits their needs. Contact us to learn more.

Further reading

- Secure and certified open source for Public Sector
- Ubuntu security certifications
- A guide to Infrastructure Hardening
- Implementing FIPS with maximum security configurations
- Introduction to cybersecurity with Ubuntu Pro on Azure Government
- Raising the bar on cybersecurity with Ubuntu for AWS GovCloud
- DISA STIG auditing and remediation in air-gapped environment
- How to enable FIPS on Ubuntu in air-gapped environments
- How Ubuntu enables your compliance with FedRAMP, FISMA, FIPS, and DISA-STIG

© Canonical Limited 2023. Ubuntu, Kubuntu, Canonical and their associated logos are the registered trademarks of Canonical Ltd. All other trademarks are the properties of their respective owners. Any information referred to in this document may change without notice and Canonical will not be held responsible for any such changes.

Canonical Limited, Registered in Isle of Man, Company number 110334C, Registered Office: 2nd Floor, Clarendon House, Victoria Street, Douglas IM1 2LN, Isle of Man, VAT Registration: GB 003 2322 47

Canonical