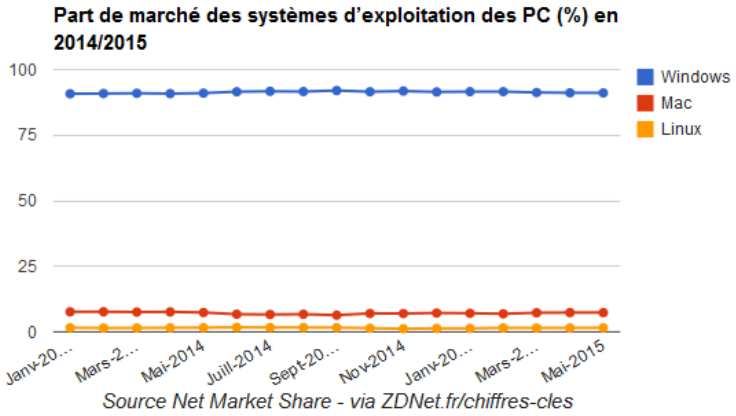
Comparatif Linux/Windows

I) Introduction

Linux est un des systèmes les plus ouverts qui soit. Chacun peut disposer des sources du noyau et des nombreux logiciels qui l'accompagnent.
Windows est une gamme de systèmes d'exploitation propriétaire produite par Microsoft, principalement destinées aux machines compatibles PC, de plus Windows est déjà installé sur les PC, ce qui ne laisse pas le choix aux utilisateurs.

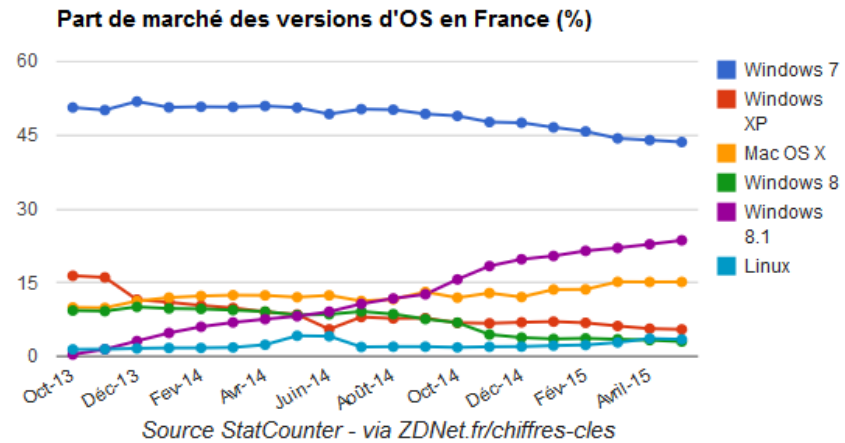
II) comparatif des OS les plus utilisés en 2014/2015 :

Dans le monde :



Source Net Market Share - via ZDNet.fr/chiffres-cles

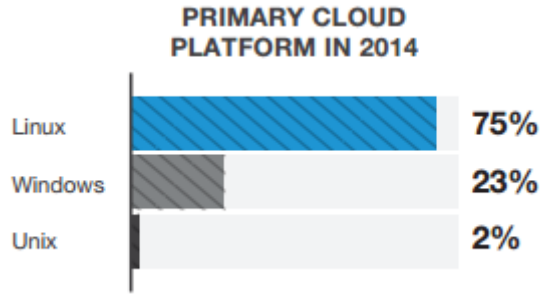
En France :



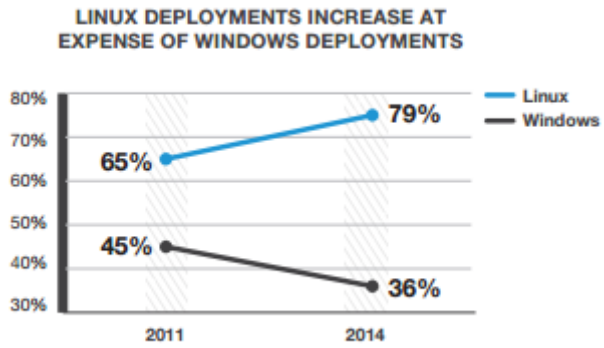
Source StatCounter - via ZDNet.fr/chiffres-cles

En entreprise

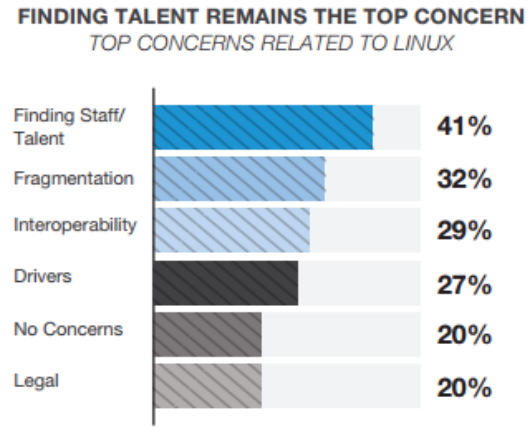
Linux équipe la plupart des serveurs web et informatiques. Les réseaux informatiques de l'Assemblée Nationale et de la Gendarmerie Nationale sont tous les deux équipés d'Ubuntu. Autant de preuves de fiabilité pour ce système d'exploitation.
Il est très répandu sur les serveurs (il est utilisé par exemple par Google et Wikipédia) et les superordinateurs.
Selon une étude publiée par l'Insee en 2011, plus de 20 % des entreprises françaises d'au moins 10 personnes auraient un ou plusieurs postes informatiques équipés d'un système d'exploitation libre (très probablement une distribution Linux).
Les OS libres sont particulièrement présents dans les entreprises qui travaillent dans le secteur de l'information et de la communication, sur 6 691 sociétés auditées, elles sont 3 817 à déclarer avoir recours à un OS libre, soit 57 % d'entre elles.
Plus l'entreprise est grande, plus l'utilisation d'au moins un poste sous Linux (ou autre système d'exploitation libre) est fréquente, jusqu'à atteindre 81 % des entreprises de moins plus de 500 salariés travaillant dans les TIC. Pour l'ensemble des entreprises de très grande taille, tous secteurs confondus, la proportion est de 55 %.
En 2014 75% des entreprises ont choisi Linux comme plate-forme de Cloud primaire en 2014, alors que les parts de Windows et Unix constituent respectivement 23% et 2%



Linux est bien meilleur en prouesses techniques et en matière de sécurité et de coût.
Les 3 principales raisons d'adapter Linux sont son ensemble de fonctionnalités (74%), la sécurité (69%), et la réduction du coût global (69%).
Ainsi, Linux continue sa croissance année après année, et cela, aux dépens de ses concurrents, Windows en particulier. En effet, selon le rapport de la Fondation Linux, de 2011 à 2014, le nombre de déploiements de Linux est monté de 65% à 79%, alors que celui de Windows a baissé de 45% à 36%.



Mais le problème est quand il s'agit de trouver des compétences Linux. Les entreprises considèrent que l'offre de talents Linux reste en dessous de leur demande, et ce problème est de plus en plus grandissant vu qu'il y a une augmentation du déploiement de la plate-forme et 41% d'entre elles sont inquiètes.



Les recruteurs recherchent tout particulièrement les profils Linux.
En 2014, 77% des responsables du recrutement ont placé dans la liste de leurs priorités l'embauche de talents Linux pour l'année à venir, contre 70% pour l'année passée. Et parmi ces 77%, plus de 9 responsables sur 10 projettent d'engager un profil Linux dans les six mois, indique le rapport relatif aux emplois Linux réalisé par la société Dice et la Fondation Linux et paru en février 2014.

III) La sécurité

L'un des arguments justifiant l'adoption de Linux par rapport aux autres plates-formes est la sécurité, et les entreprises l'ont clairement exprimé avec un taux de 75%.
Un bon programmeur peut traquer les bugs, inclure des améliorations, modifier les sources, compiler tout ou une partie du système Linux.
Cette disponibilité des sources a deux effets sur la sécurité : un bon hacker peut trouver un bug dans une source susceptible d'être utilisé pour déstabiliser ou attaquer le système. Il est probable qu'il décidera d'en avertir la communauté Linux et proposera parfois un correctif. C'est l'aspect positif des choses : le noyau ou le programme incriminé sera rapidement corrigé et la sécurité accrue. Mais il y a certaines personnes qui vont pouvoir exploiter ce bug, pendant quelques temps, afin de s'introduire sur des systèmes, c'est le côté négatif.
Les différents moyens de communication (protocoles, programmes, …) sont à l'origine de failles de sécurité. En effet, pour communiquer, ils ouvrent des voies de communication qui, si elles ne sont pas bien contrôlées, sécurisées, peuvent représenter une porte d'entrée à des intrusions et des attaques.

- Par défaut, les utilisateurs de Linux n'ont pas les droits administrateur, et ne peuvent donc pas modifier les fichiers système. Donc difficile pour un virus d'infecter la machine.
- GNU/Linux vous oblige à déclarer si un fichier est exécutable ou non. Impossible d'être infecté par *pamela.jpg.exe* en pensant que c'était une image.
- La configuration par défaut de Linux est généralement plus sûre que celle de Windows (*il y a généralement assez peu de services réseau ouverts, voire pas du tout (comme dans Ubuntu)*).
- Les failles sont généralement plus vite corrigées *(Microsoft a mis plusieurs mois à corriger certaines failles, et a même dû en corriger certaines sous la menace (cf. les failles dénoncées par eEye Security.)*)
- Le fait que GNU/Linux soit open source fait que tout le monde peut examiner le code source, y compris divers experts en sécurité. Il y a donc plus d'yeux pour examiner les sources de Linux que, probablement Windows. Les failles ont donc plus de chances d'être détectées.

- Les utilisateurs de Linux téléchargent généralement leurs logiciels dans des dépôts de logiciels dont le contenu est contrôlé. Il y a rarement besoin de prendre des logiciels hors de ces dépôts, et donc moins de risques de tomber sur un site douteux. Avec Windows, il faut tout aller télécharger sur divers sites, et s'assurer qu'un site de téléchargement est sain n'est pas toujours facile.
- Enfin, il existe une grande variété de distributions Linux différentes. Elles sont toutes légèrement différentes, ce qui rend la vie des virus beaucoup plus difficile.

Tout cela fait que Linux est naturellement moins sujet aux virus. Mais cela ne veut absolument pas dire qu'il y soit totalement invulnérable.
La plupart des utilisateurs de Linux se pensent protégés, même si cela est en grande partie vrai, quelques virus font leur apparition et donc recourir à un antivirus pour assurer sa protection parait toutefois judicieux.
De même si vous transférez des fichiers de GNU-Linux sur un autre système d'exploitation celui-ci qui est inactif sur GNU/Linux pourra l'être sous un autre système d'exploitation.
De même, si vous utilisez un logiciel de virtualisation les risques ne sont pas négligeables.
Les solutions pour se protéger :

- Un anti-virus
- Un Parefeux
- Un logiciel de nettoyage

Sécuriser un serveur Linux

Par définition, un serveur est ouvert sur le monde, un minimum de sécurité est donc intéressant afin de se prémunir des attaques les plus simplistes.

- Filtrer le trafic via le firewall
- Déclaration des règles : filtrage intégral en créant un script
- Ouvrir les ports utilisés
- Scanner les ports
- Bannir des IP
- Détecter les intrusions avec un logiciel
- Détecter les rootkits
- Surveiller les Logs
- Utiliser un anti-spam pour les mails
- chercher les failles de la machine

90 % des problèmes informatiques relèvent de l'utilisateur. C'est pourquoi, avant même de penser à sécuriser sa machine, il faut garder en mémoire quelques règles de bon sens :

- interdire les utilisateurs sans mot de passe (ce sont d'énormes failles potentielles)
- toujours choisir de bons mots de passe
- maintenir son système à jour.
- toujours utiliser ssh pour l'accès à distance (et non telnet ou des services graphiques, sauf s'ils sont en tunnel à travers ssh).

Les Virus et Linux sur Serveur

Souvent appelés Rootkits. Un Rootkit n'est pas un Virus, mais un logiciel injecté par un pirate dans un serveur ayant une faille de sécurité permettant d'exécuter du code non sollicité. Un Rootkit permet de sécuriser le chemin permettant à un pirate de faire plus ou moins n'importe quoi avec le serveur. Pour être infecté par un Rootkit il faut pouvoir y accédé de l'extérieur.

Comparatifs des différents OS concernant les failles de sécurités en 2014 :

Operating system	# of vulnerabilities	# of HIGH vulnerabilities	# of MEDIUM vulnerabilities	# of LOW vulnerabilities
Apple Mac OS X	147	64	67	16
Apple iOS	127	32	72	23
Linux Kernel	119	24	74	21
Microsoft Windows Server 2008	38	26	12	0
Microsoft Windows 7	36	25	11	0
Microsoft Windows Server 2012	38	24	14	0
Microsoft Windows 8	36	24	12	0
Microsoft Windows 8.1	36	24	12	0
Microsoft Windows Vista	34	23	11	0
Microsoft Windows RT	30	22	8	0

IV) Les logiciels

La plupart des logiciels fonctionnants sous Windows ont des alternatifs sous Linux et très souvent gratuit par exemple toute la suite Office de Microsoft qui est payante n'est pas sous Linux mais il y a LibreOffice qui fait les même fonctions, qui est gratuit et dont les formats d'enregistrements sont compatibles Windows.
Un autre exemple qui lui est compatible Linux alors que c'est la propriété de Microsoft : Skype
Pour les navigateurs internet il y a aucun souci, Firefox et Opera (par exemple) marche sous Linux et Windows.

On peut aussi utiliser le logiciel Wine sous Linux qui permet de faire fonctionner des logiciels pour Windows. Contrairement à VMWare ou VirtualBox, Wine n'émule pas un PC complet, mais seulement les API Win32 (appels système Windows).
L'émulation n'est pas parfaite, mais elle permet dans bien des cas de faire fonctionner des applications Windows directement sous Linux, sans avoir recours aux lourdes machines virtuelles.
Il est quand même préférable d'utilisé des logiciels pour Linux qui permettent de faire les mêmes fonctions qu'un logiciel sous Windows.

V) Gestion des groupes et utilisateurs

Linux est, comme d'autres systèmes, multi-utilisateurs. Ceci signifie qu'il sait gérer des sessions distinctes pour plusieurs utilisateurs de la machine qui auront leur accès propre. Cet accès personnalisé se fait en général par le biais de login et password, ce qui est assez standard. Dans sa session, un utilisateur peut accéder à un répertoire qui lui sera dédié (en général /home/nom_utilisateur, mais cela peut être modifié par l'administrateur). Il pourra faire tout ce qu'il voudra dans cette espace dédié, même complètement détruire son compte, c'est-à-dire effacer complètement le répertoire, sous-répertoires et fichiers cachés compris. Il est également possible de naviguer à certains endroits de l'arborescence de la machine à laquelle il s'est connecté. Il peut aussi lancer des applications déjà installées sur la machine, créer et exécuter ses propres scripts ou programmes. Mais la liberté de l'utilisateur a ses limites, celles imposées par l'administrateur (ou par un autre utilisateur pour les fichiers lui appartenant).

Chaque élément du système et de la machine est considéré comme un fichier avec des droits d'accès bien définis. Un utilisateur ne pourra pas accéder à un répertoire, un lecteur cd ou autre binaire si les permissions attribuées ne l'y autorisent pas.

VI) Contrôleur de domaine

Le logiciel Samba : sa fonction est de partager des dossiers et des imprimantes à travers un réseau local.
Il permet de partager et d'accéder aux ressources d'autres ordinateurs fonctionnant avec des systèmes d'exploitation Windows et Mac OS X, ainsi que des systèmes GNU/Linux, BSD et Solaris dans lesquels une implémentation de Samba est installée.
Grace à ce logiciel on peut mettre en place un contrôleur de domaine.

SAMBA est donc un outil réseau performant afin de communiquer avec le monde Windows depuis Linux.

VII) Conclusion

Linux est un OS très performant et surtout que la plupart des distributions sont gratuites.
Il peut très bien remplacer Windows pour un utilisateur non professionnel puisqu'il y a l'équivalent de la plupart des logiciels utilisé pour Microsof.
Je conseille Linux pour les serveurs Web pour sa gratuité, sa puissance suffisante, sa licence libre et surtout pour sa sécurité.

Sources :

ubuntu-fr
Linux Foundation
Numerama
open-source-guide