Votre windOwS est-il un risque pour votre entreprise?

Luc Pierson
Sortir Du Brouillard Informatique
luc.pierson@sdbinfo.fr
06 37 55 33 56

20 Novembre 2025

version 1.0

Agenda

- Disclaimer
- Introduction
- Historique - Windows XP à aujourd'hui
- Pourquoi ? Des problèmes structurels
- Changer face à la réalité de terrain
- Les Alternatives
- Conclusion

“Notre rapport à la technologie est maintenant est quasi magique.

Notre crasse ignorance (et en particulier des OS)
ne nous fait pas trembler d’angoisse ou rougir de honte.

Mais avons-nous raison de rester un public fantôme ?”

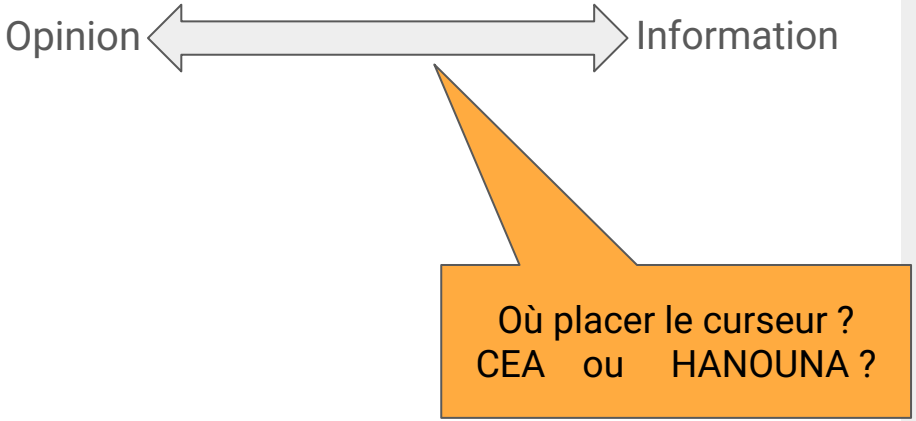
Librement inspiré d’une conférence d’Etienne KLEIN

Pourquoi je suis devant vous ?

- Smalltalk => dev et portage
- Ecran Bleu en conférence

Disclaimer

Windows Pros & Cons : un sujet clivant



Qui est assez expert ?
Sur quelle notion baser son observation ?

- Adoption
- Désir des utilisateurs
- Facilité de prise en main
- Outlook/Word/Excel
- Temps perdu à réparer
- Nombre de failles
- Le coût des failles
- Nombre d'attaques
- Nombre de contributeurs
- Propriété technologique
- etc…

Windows, obsolescence programmée ?

Il faut rester raisonnable

OUI
Microsoft n’est pas une société philanthropique et défend ses intérêts tout en restant en position hégémonique sur les PC.

NON
Microsoft n’a aucun intérêt à perdre ces usagers, mais souhaite limiter les coûts de maintien en conditions opérationnelles des multiples variantes de Windows

pas délibérément…

« Je souhaite aujourd'hui aborder un sujet essentiel pour l'avenir de notre entreprise : donner la priorité à la sécurité avant tout le reste »…

Introduction à un Mémo en 2024 par Satya Nadella
Microsoft impose une "nouvelle" culture interne qui place la sécurité en premier avec son initiative Secure Future Initiative (SFI),

« Si vous devez choisir entre la sécurité et une autre priorité, la réponse est claire : privilégiez la sécurité. Dans certains cas, cela signifie qu'il faut **donner la priorité à la sécurité plutôt qu'à d'autres choses, comme le lancement de nouvelles fonctionnalités ou la continuité d'activité de systèmes ancestraux**. Il s'agit là d'un élément clé pour faire progresser à la fois la qualité et les capacités de nos plateformes afin de protéger les biens numériques de nos clients et de construire un monde plus sûr pour tous »

May 3rd, 2024
https://blogs.microsoft.com/blog/2024/05/03/prioritizing-security-above-all-else/

Introduction

Mai 2017 - WannaCry ransomware cryptoworm

- faille du protocole de partage de fichiers et d'imprimantes de Windows
- problème connu et exploité par la NSA depuis XX années (connu sous le pseudo EternalBlue)
- chiffrage des fichiers et demande de rançon par les escrocs
- Impact
  - NHS (système de santé britannique) : hôpitaux paralysés, opérations annulées.
  - Renault-Nissan : usines temporairement à l'arrêt.
  - FedEx, Telefonica, Deutsche Bahn, Ministère de l'Intérieur russe, etc.

- **Microsoft avait publié un correctif de sécurité (MS17-010) dès mars 2017, deux mois avant l'attaque, mais beaucoup de systèmes ne l'avaient pas (ou pas encore) appliqué.**

Anecdote

le robot de sauvegarde d'une usine à Belfort

WannaCry ransomware cryptoworm

Qui en profite, au niveau Externe ?

- **groupe Lazarus**, lié à la **Corée du Nord**.
- **gain : MM$**

Qui en profite, au niveau Interne ?

- **Le confort de quelques un(e)s : “j’y suis habitué (e), je ne souhaite pas changer !**
- **Tout le monde fait comme cela**
- **Les éditeurs proposent seulement leur logiciel solution sur cet OS**

Réponse 1

- **Mises à jour de sécurité régulières** (en particulier // sécurité)
- Réaliser des **Sauvegardes hors ligne**.
- Garder un œil expert pour avoir une conscience accrue des **risques liés aux ransomwares**, voire monter une team experte en Sécurité des SI

Réponse 2

- Envisager une **refonte des systèmes et des usages.**

Autres failles historiques majeures

Date	Faille	Impact	Coût estimé
Août 2003	**Blaster (MS03-026)**	16 millions de PC, arrêt d'usines	2-10 milliards $
Mai 2017	**WannaCry (EternalBlue)**	200 000 PC, NHS britannique paralysé	4 milliards $
Juin 2017	**NotPetya**	Maersk, Merck, FedEx à l'arrêt	10 milliards $
Mars 2021	**ProxyLogon (Exchange)**	30 000 serveurs Exchange compromis	Non chiffré
Juillet 2024	**CrowdStrike (pilote kernel)**	8,5 millions de PC, chaos mondial	10 milliards $

Des centaines d’attaques tous les ans

Windows est une cible idéale

Problèmes structurels

Problème du nombre de déploiements auprès de personnes peu désireuses d’aller au-delà de leur simple usage

Historique - Windows XP à aujourd'hui

20 ans de promesses non tenues

Windows XP (2001-2014)

Le mythe : "Le Windows le plus stable"

La réalité :

- Kernel NT 5.1 - architecture 32 bits limitée
- Faille Blaster (2003) : 16 millions de PC infectés
- Support prolongé jusqu'en 2014 par manque d'alternative viable

Windows Vista (2007-2017)

Le désastre public

- Kernel NT 6.0 - réécrit partiellement, instable
- UAC (User Account Control) : sécurité intrusive mais inefficace
- Incompatibilité massive avec les pilotes et logiciels XP
- Configuration requise excessive pour l'époque

Chiffre : 2009 - Seulement 20% de parts de marché, alors que XP gardait 62%

Windows 7 (2009-2020)

Le "sauveur" : en fait, juste Vista réparé

- Kernel NT 6.1 - même base que Vista, corrigé
- Meilleure gestion mémoire, mais toujours 4GB RAM max en 32 bits

Date clé : Janvier 2020 - Fin du support, 26% des PC professionnels encore sous W7

Windows 8/8.1 (2012-2023)

L'erreur stratégique

- Interface Metro : imposée, inadaptée au desktop
- Suppression du menu Démarrer (restauré en 8.1)
- Adoption catastrophique : 6% de parts de marché maximum

Windows 10 (2015-2025)

"La dernière version de Windows" (dixit Microsoft en 2015)

- Kernel NT 10.0
- Mises à jour forcées catastrophiques (pertes de données, bugs)
- Mai 2019 : Update 1903 supprime des fichiers utilisateurs
- Octobre 2018 : Update 1809 retiré après 48h pour bugs critiques
- Télémétrie invasive impossible à désactiver complètement

Date clé : Octobre 2025 - Fin du support annoncée (puis repoussée)

Windows 11 (2021-aujourd'hui)

L'obsolescence matérielle forcée

Exigence TPM 2.0 : élimine des millions de PC fonctionnels
Kernel NT 10.0 (identique à W10, juste renuméroté en marketing)
Interface redessinée : ralentissements sur matériel récent
Incompatibilité artificielle avec CPU < 8ème gen Intel (2017)

Tech & web

En un claquement de doigts, près de 400 millions d'ordinateurs dans le monde sont devenus caducs le 14 octobre 2025, d'après les calculs de l'association Halte à l'Obsolescence Programmée. En cause? La décision du géant du numérique Microsoft de cesser les mises à jour de sécurité sur son système d'exploitation Windows 10. Elle force ainsi le passage à Windows 11 pour ne pas s'exposer au risque de cyberattaques.

https://www.lefigaro.fr/secteur/high-tech/obsolescence-de-windows-10-le-figaro-a-teste-durant-un-mois-le-passage-au-systeme-d-exploitation-libre-linux-20251115

Petit exemple récent

on parle de l'update 24H2 ?
des heures de réparation pour relancer des installations complètes ?

Pourquoi ? Des problèmes structurels

Problèmes du noyau Windows :

La Registry : un point de défaillance unique

- Base de données centralisée qui se corrompt
- Fragmentation progressive inévitable

Aucun équivalent sous Linux/MacOS (fichiers texte distribués)

La gestion mémoire déficiente

- Memory leaks non nettoyés
- Swap (fichier d'échange) qui sature le disque

Linux : gestion mémoire optimisée depuis des décennies

Le mode Ring 0 trop accessible

- Pilotes en mode kernel = instabilité totale
- Un pilote graphique qui plante = écran bleu

Linux : pilotes isolés, MacOS : validation stricte

Illustration datée :

- **Juillet 2024** : Incident CrowdStrike - un seul fichier de pilote défectueux met hors service 8,5 millions de PC Windows mondialement (compagnies aériennes, hôpitaux, banques). Coût estimé : 10 milliards $
- **Pourquoi pas d'impact CrowdStrike sur Linux/Mac ?** Ces systèmes isolent les pilotes, l'impact aurait été limité

La Compatibilité Ascendante : Un Boulet

Le mythe : "Windows fait tourner vos vieux logiciels"

En réalité : **Applications 32 bits sur Windows 64 bits**

- Couche WoW64 (Windows on Windows) : traduction à la volée = perte de performance
- Bibliothèques DLL multiples versions qui se télescopent
- "DLL Hell" : conflits entre versions de bibliothèques

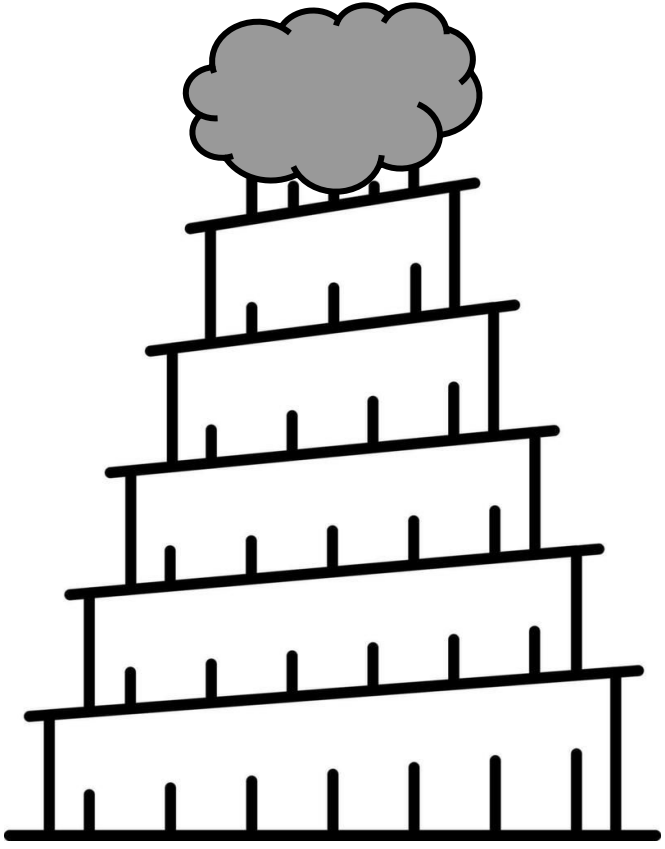
En réalité : Les modes de compatibilité = rustines

- Windows XP Mode dans W7 : machine virtuelle cachée, lente
- Windows 10 "mode compatibilité" : 15 options différentes qui ne fonctionnent que aléatoirement

Exemple concret :

- **2021** : Adobe arrête le support 32 bits, des milliers d'entreprises bloquées
- **Depuis 2003**, mai reforcé depuis w7, besoin d'outils de nettoyage de registres et de DLLs externes (CCleaner)

C. .NET et les Frameworks : La Tour de Babel



2023 : .NET 8

2022 : .NET 7

2021 : .NET 6

2020 : .NET 5 (fusion annoncée de .NET Framework et Core)

2019 : .NET Core 3.0

2016 : .NET Core 1.0 **(nouvelle branche incompatible)**

2012 : .NET Framework 4.5

2010 : .NET Framework 4.0 **(incompatible avec 3.x)**

2007 : .NET Framework 3.5

2006 : .NET Framework 3.0 **(requiert 2.0)**

2005 : .NET Framework 2.0 **(incompatible avec 1.0)**

2002 : .NET Framework 1.0

Changer face à la réalité de terrain

Oui, mais 1/2

1. Compatibilité des Applications

De nombreux logiciels professionnels et spécialisés (Adobe Creative Suite, AutoCAD, logiciels métiers spécifiques) sont développés exclusivement pour Windows.

Alternatives

- Presque tous les logiciels ont une alternative open-source, Si un logiciel vous force dans la présentation, c'est une maturité de l'éditeur à remettre en question.
- Le Cloud et l'appui sur les navigateurs moyennent à la baisse ce besoin.
- Envisager Windows uniquement pour usage spécifique

2. Coût et complexité de la migration

Remplacer Windows dans une organisation représente un investissement considérable : migration des données, adaptation des processus, support technique. Ces coûts directs et indirects peuvent être dissuasifs, surtout pour les PME.

Faux

- Avec une architecture du SI conçue sur des solutions stables avec peu d'adhérence aux systèmes.
- Ne pas confondre architecture du SI et Microsoft.
- Se recentrer sur des solutions cœur de métier permet de minimiser le coût du changement

Oui, mais 2/2

3. Habitudes et courbe d'apprentissage Les utilisateurs ont souvent des années d'expérience avec Windows. Changer de système d'exploitation nécessite un réapprentissage qui peut temporairement réduire la productivité et générer des résistances au changement.

Accompagnement au changement
Déjà nécessaire déjà dans un changement de Windows X à Windows Y et à ne pas minimiser. Toutefois, envisager que ce soit moins souvent…

4. Support matériel et périphériques Windows bénéficie d'un support matériel quasi universel. Imprimantes, scanners, webcams et autres périphériques fonctionnent généralement "out of the box".

Sujet devenu trop rare pour s'y attarder,
⇒ y être attentif et challenger ses fournisseurs, un gain de temps sur l'obsolescence mérite un peu d'attention

5. Écosystème et intégration L'intégration avec Active-Directory, les stratégies de groupe, Microsoft 365, et l'ensemble de l'écosystème Microsoft crée une dépendance forte. Reproduire cette intégration avec d'autres solutions demande expertise et ressources.

Vous dépensez déjà cet argent, mais c'est à MS que vous le donnez…
Savez-vous que Windows dans le cloud tourne sous Linux (Azure = 60% Linux)?

Alternatives

LES ALTERNATIVES VIABLES:

Pour les Stations de travail

iOS / MacOS

Kernel XNU (basé sur Mach + BSD Unix)

- Stabilité prouvée depuis 2001
- Gestion mémoire optimale
- Uptime moyen : 6-12 mois sans reboot
- **Securité** Gatekeeper : validation des applications
- SIP (System Integrity Protection) : système de fichiers protégé
- Sandboxing obligatoire pour App Store

Statistiques :

- **Gartner 2023** : 23% des entreprises équipent leurs employés en Mac
- **IBM 2023** : 290 000 Mac déployés, coût de support 3x inférieur à Windows

Inconvénients :

- Prix du matériel
- Lock-in Apple
- Moins de logiciels spécialisés (mais en diminution)

Android / Linux / ChromeOS

Adoption entreprise (Linux):

- **Google** : 100% des employés sur Linux
- **SpaceX** : stations de contrôle sur Linux
- **CERN** : scientifiques sur CentOS/RHEL (Red Hat Linux)

Avantages utilisateur :

- Gratuité ou abonnements maîtrisée (TCA/TCO réduit)
- Pas d'obsolescence forcée
- Hardware ancien supporté (10+ ans)
- Personnalisation totale

Inconvénients :

- Certains logiciels professionnels absents (Adobe suite)
- Support matériel parfois retard

Illustration : **Baccarat, 2006**

LES ALTERNATIVES VIABLES :

Pour les serveurs

Type d'infrastructure	Part de marché Linux	Date
Top 500 Supercalculateurs	100%	2023
Serveurs web	77.7%	2024
Cloud AWS	~92% instances	2023
Serveurs d'entreprise	70%	2024

Illustration : **ATOS BDS**

Linux pour les infrastructures critiques

Stabilité

- Kernel modulaire, extensible sans reboot
- Uptime record : serveurs avec 10+ ans sans reboot
- Mises à jour sécurité sans interruption (KernelCare, kpatch)

Sécurité

- Open source : audité par des milliers de développeurs
- SELinux/AppArmor : contrôle d'accès obligatoire
- Principe du moindre privilège par défaut

Performance

- Gestion mémoire optimale (cache, buffers)
- Ordonnancement de processus supérieur
- Pas de "bloatware**"

** Les logiciels préinstallés, résidents, aussi appelés **«bloatware»**: les applications ou programmes souvent préinstallés sur un appareil par le fabricant ou l'opérateur ou l'éditeur.
Traductions usitées : mémorivore, inflagiciel, obésiciel ou boufficiel

Exemples d'usages - Linux

Solutions NAS professionnelles

- Synology : Linux (DSM sur Debian)
- QNAP : Linux (QTS)
- TrueNAS : FreeBSD/Linux
- **Aucun sur Windows**

Conteneurs et Orchestration

- Docker : Linux (nativement)
- Kubernetes : Linux
- Windows: 5% de part de marché

Appliances de Sécurité

- Pare-feu : pfSense (FreeBSD), OPNsense, Fortinet (Linux)
- Proxy : Squid, HAProxy (Linux)
- IDS/IPS : Snort, Suricata (Linux)
- **Aucun sur Windows**

Serveurs Web et Bases de Données

- Apache, Nginx : Linux (98% des déploiements)
- MySQL, PostgreSQL, MongoDB : Linux
- Redis, Elasticsearch : Linux

Routeurs et Switches

- Cisco IOS : Unix-like
- Juniper JunOS : FreeBSD
- MikroTik RouterOS : Linux
- **Aucun sur Windows**

Microsoft

- Microsoft Cloud Azure : 60% sur Linux
- **GitHub** : infrastructure Linux
- **WSL2** (Windows Subsystem for Linux) :
  Microsoft : "Pour développer,
  il vaut mieux Linux sous Windows !"

Conclusion

Un peu de clivage

1. "L'obsolescence de Windows n'est pas un bug, c'est un “business-modèle”.

2. Chaque nouvelle version est une promesse de résoudre les problèmes de la précédente, alors que les problèmes sont dans les fondations.

3. Ceux qui misent leur business sur la fiabilité ont choisi : ils n'utilisent pas Windows pour ce qui compte.

Pour paraphraser EK : **“S’indigner assis sur son canapé, ce n’est pas très utile”**

Convictions ?

Si votre business
= f(obsolescence de votre informatique)
= f(Version du système Windows)

alors que pouvez-vous conclure ?

Les vrais coûts cachés ?

- Passer de Windows 10 à Windows 11 ? **C'est une migration technique + un remplacement de certains matériels + des prestations d'informaticiens + un accompagnement au changement des utilisateurs.**

- L'audit annuel des licences pour être "en règle" ? C'est de l'anxiété institutionnalisée.

- La compatibilité d'Outlook/Word/Excel? C'est du verrouillage déguisé en confort.

- Migrer vers l'open-source, c'est aussi une migration ! Mais cela pourrait être la dernière.

Proactif ? d'accord

mais….par où je commence ?

- J'apprends à dominer mon accoutumance à Excel et à Outlook
- J'étudie mes besoins actualisés, le OS au bon endroit, quels usages, quelles contraintes
- Je garde mes OS à jour
- C'est moi le boss, pas les "fournisseurs" :
  - Les éditeurs me doivent une version fonctionnelle et testée **AVEC** les derniers patchs de sécurité
- Ma valeur IT == mes données :
  - Je sauvegarde (321) et je teste ma capacité à reprendre ("PRA" full ou en dégradé).
  - Je libère au maximum mes données des logiciels qui les gèrent
- J'appelle un professionnel pour m'accompagner et travailler sereinement

Pas Urgent…	…mais quand même **Stratégique**

www.sdbinfo.fr

Votre partenaire : **Luc PIERSON**
Architecte Informatique
DSI virtuelle
email : luc.pierson@sdbinfo.fr
06 37 55 33 56

MERCI

Quelques sources

- Microsoft Security Response Center (MSRC) - historique CVE
- Gartner Market Share Reports (2020-2024)
- Incident CrowdStrike - Rapport Microsoft (juillet 2024)
- WannaCry/NotPetya - Rapports Europol, FBI (2017-2018)
- Top500.org - Statistiques supercalculateurs
- W3Techs - Parts de marché serveurs web
- IBM Mac@IBM Reports (2019-2023)

Inspiration

- Le « halo symbolique » des nouvelles technologies | Étienne Klein | Université de Strasbourg | 20 Oct 2021