O'REILLY®
Report

Repenser le choix du système d'exploitation

Quand la stratégie Linux devient un avantage concurrentiel

Ned Bellavance et Chris Hayner

Offert par

Red Hat

Red Hat Enterprise Linux

Choisissez un système d'exploitation qui donne un avantage concurrentiel

Accélérez l'innovation grâce à une plateforme moderne. Découvrez comment Red Hat Enterprise Linux vous offre le niveau nécessaire d'agilité et de contrôle pour vous adapter à l'évolution de la demande.

En savoir plus

Repenser le choix du système d'exploitation

Quand la stratégie Linux devient un avantage concurrentiel

Ned Bellavance et Chris Hayner

O'REILLY®

Repenser le choix du système d'exploitation
par Ned Bellavance et Chris Hayner

Publié par O'Reilly Media, Inc., 141 Stony Circle, Suite 195, Santa Rosa, CA 95401, États-Unis.

Les livres O'Reilly peuvent être achetés à des fins éducatives, commerciales ou promotionnelles. Des éditions en ligne sont également disponibles pour la plupart des titres (*http://oreilly.com*). Si vous souhaitez plus d'informations, contactez notre service commercial pour les entreprises et les organismes : 800 998 9938 ou *corporate@oreilly.com*.

Éditrice des acquisitions : Megan Laddusaw
Responsable éditorial : Gary O'Brien
Assistant éditorial : Jonathon Owen
Relectrice-correctrice : Stephanie English
Graphiste (couverture) : Ellie Volckhausen
Graphiste (intérieur) : David Futato
Illustratrice (intérieur) : Kate Dullea

Février 2026 : première édition

Historique des révisions pour la première édition
13/02/2026 : première version

Le logo O'Reilly est une marque déposée d'O'Reilly Media, Inc. *Repenser le choix du système d'exploitation*, l'image de couverture et l'habillage commercial associé sont des marques d'O'Reilly Media, Inc.

Ce document s'inscrit dans une collaboration entre O'Reilly et Red Hat. Veuillez consulter la déclaration d'indépendance éditoriale.

979-8-341-66786-0

[LSI]

Sommaire

Introduction

Les entreprises ont toujours tardé à changer de stratégie de déploiement des systèmes d'exploitation. Elles s'appuyaient sur des exigences techniques simples et des préférences établies et n'exécutaient plusieurs systèmes d'exploitation qu'en cas de nécessité absolue. Les changements étaient généralement dictés par les besoins techniques d'une application essentielle ou par l'obsolescence d'un système arrivé en fin de prise en charge. Pour les entreprises, le choix du système d'exploitation ne représentait donc guère plus qu'une contrainte technique. Cependant, la vitesse d'évolution du paysage technologique mondial transforme aujourd'hui cette décision en impératif stratégique.

Les entreprises évoluent désormais dans un environnement marqué par des changements bien plus rapides que par le passé. En quelques années seulement, les technologies telles que la conteneurisation ont amélioré la flexibilité des workflows, les ensembles d'outils et les stratégies pour le déploiement d'applications ont radicalement changé et les technologies comme l'IA et l'informatique quantique ont totalement bouleversé nos repères. Dans ce contexte instable, les entreprises doivent non seulement réévaluer leurs besoins en technologies, mais aussi repenser leurs critères de choix en matière de système d'exploitation.

Ce rapport analyse les facteurs à l'origine de ce nouvel impératif stratégique. Il s'appuie sur des recherches empiriques, notamment des enquêtes et des rapports d'analyste, pour identifier les défis spécifiques auxquels sont confrontées les équipes informatiques modernes. Cette évolution semble venir d'un certain nombre de déclencheurs stratégiques apparus très récemment. Les nouvelles applications, les

infrastructures matérielles et les plateformes s'inscrivent dans une dynamique d'accélération de l'innovation. En parallèle, les entreprises doivent composer avec un contexte économique incertain, des cybermenaces modernes et sophistiquées, ainsi que des enjeux géopolitiques tels que la souveraineté des données et la validation des chaînes d'approvisionnement.

Ce rapport montre comment les entreprises redéfinissent la sélection du système d'exploitation en la considérant non plus comme une contrainte opérationnelle, mais comme un avantage concurrentiel stratégique.

CHAPITRE 1

Un changement stratégique dans le choix du système d'exploitation

Les exigences liées aux environnements informatiques modernes transforment en profondeur l'infrastructure du système d'exploitation et la stratégie de déploiement des applications. Les entreprises qui ne changeaient ni ne remettaient jamais en question leur système d'exploitation réévaluent la pertinence de cette approche (simplification de la gestion et du déploiement, réduction du besoin de formation, etc.) face à la rapidité actuelle des progrès. Elles prennent conscience que leur tendance à l'immobilisme représente un frein plutôt qu'un atout. La flexibilité et la capacité d'évolution rapide deviennent des priorités, au détriment du maintien du statu quo. Les entreprises qui n'envisagent pas cette voie risquent de se laisser dépasser par des concurrents mieux préparés qui s'adaptent plus facilement. Par ailleurs, à la rapidité des changements technologiques s'ajoutent certains facteurs géopolitiques qui influencent directement les décisions en matière d'approvisionnement.

Principaux facteurs et changements

Le choix du système d'exploitation s'appuie désormais sur plusieurs facteurs. Il ne s'agit pas de tendances isolées, mais de forces interconnectées qui redéfinissent les stratégies d'infrastructure. Ces différents facteurs seront détaillés dans la suite du rapport.

L'*accélération de l'innovation* est le premier critère de sélection du système d'exploitation. L'IA, l'automatisation, l'edge computing et le cloud computing, l'IoT (Internet des objets) et les nouveaux équipements matériels personnalisés évoluent à une vitesse telle que toutes les entreprises ne peuvent pas suivre le rythme. Elles craignent

que cette évolution sans précédent entraîne une dette technique importante. Avant, il fallait des années pour qu'une technologie émergente passe en production, alors qu'aujourd'hui quelques mois suffisent. C'est principalement pour cette raison que les entreprises recherchent aujourd'hui un système d'exploitation qui leur permet de rester compétitives.

L'*incertitude mondiale* relative aux chaînes d'approvisionnement augmente depuis quelques années. Les entreprises élargissent leur analyse au-delà de leur environnement immédiat pour prendre en compte l'ensemble des acteurs impliqués dans la fourniture des outils, logiciels et services. En raison des perturbations qui pourraient survenir dans la chaîne d'approvisionnement, beaucoup d'entreprises estiment qu'il est devenu risqué de compter sur un fournisseur unique, en particulier si celui-ci se trouve à l'étranger. Ces inquiétudes ont donné lieu à une diversification des fournisseurs, un impératif stratégique visant à atténuer les risques.

Les *pressions économiques* se sont intensifiées, notamment au niveau de l'optimisation et du retour sur investissement (ROI). Ce dernier ne se limite pas aux aspects financiers : le manque de compétences est aussi important que les contraintes budgétaires, ce qui complique le choix du système d'exploitation. Avant, un seul administrateur maîtrisait rarement parfaitement plusieurs systèmes d'exploitation, mais il n'était pas envisageable de recruter plusieurs spécialistes de haut niveau. C'est l'une des raisons pour lesquelles les entreprises se contentaient généralement d'un seul système d'exploitation. Dans ce contexte, la facilité d'utilisation devient un critère de choix déterminant.

Les *préoccupations liées à la sécurité* ont redéfini les exigences en matière d'infrastructure. Les entreprises déploient de plus en plus de systèmes, ce qui étend considérablement leur surface d'attaque. Avec l'adoption de l'IA, l'apparition de cybermenaces modernes et l'évolution de la conformité réglementaire, il est temps d'envisager de nouvelles approches.

Enfin, l'*IA* a révolutionné l'utilisation des ordinateurs. Les équipes d'administration et de développement peuvent créer des applications à une vitesse sans précédent grâce aux grands modèles de langage (LLM). Qu'il s'agisse d'interagir avec un LLM, de concevoir un dialogueur (ou chatbot) ou de développer des solutions d'IA

agentique avancées, le choix du système d'exploitation devient un facteur clé de réussite.

Importance du choix du système d'exploitation

Comme nous l'avons vu, la sélection du système d'exploitation repose aujourd'hui sur un ensemble de facteurs bien plus large qu'auparavant. Un mauvais choix peut limiter l'accès aux fonctionnalités d'IA essentielles, nuire aux performances et exposer les entreprises à des risques pour la sécurité ou à des vulnérabilités au niveau de la chaîne d'approvisionnement. À l'inverse, le bon système d'exploitation peut devenir un tremplin vers la réussite dans un monde à l'évolution effrénée, axé sur la productivité. Un choix stratégique et rigoureux permet aux entreprises de bénéficier d'un avantage concurrentiel et d'une flexibilité numérique, et ainsi de tirer parti des nouvelles technologies.

Examinons à présent ces différents facteurs plus en détail.

Accélération de l'innovation

Le rythme soutenu des avancées technologiques a profondément transformé les modèles traditionnels de prise de décision en matière d'infrastructure. Cette section présente les moteurs d'accélération à l'œuvre et la manière dont les entreprises adaptent leurs stratégies de déploiement en conséquence.

Cycles technologiques accélérés

Comme l'indique le rapport McKinsey Technology Trends Outlook pour 2025, le paysage technologique mondial connaît des transformations majeures, portées par des innovations rapides[1]. En d'autres termes, les développements technologiques s'opèrent à un rythme inédit, appelé à s'intensifier. À titre d'exemple, l'adoption du cloud s'est souvent faite de manière progressive : les entreprises ont d'abord déployé des environnements de développement et de test, avant de migrer des charges de travail en production sur plusieurs

[1] McKinsey & Company, « McKinsey Technology Trends Outlook 2025 », 22 juillet 2025, *https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top- trends-in-tech*.

années. En revanche, pour les innovations plus récentes, comme l'IA générative ou agentique, le passage du stade conceptuel à des applications en entreprise n'a pris que quelques mois.

Dans le cadre d'une stratégie d'infrastructure classique, les entreprises utilisent leur système d'exploitation existant et trouvent un moyen d'y intégrer les nouvelles technologies. Cette approche n'est toutefois plus suffisante au vu de la rapidité du marché mondial moderne. Au lieu d'essayer d'accommoder leur ancienne infrastructure, les équipes de développement modernes testent de nouvelles plateformes pour trouver les plus adaptées aux dernières technologies. Cette dynamique favorise l'expérimentation autour des systèmes d'exploitation : lorsque le système en place ne répond plus aux attentes des équipes de développement et d'ingénierie, la recherche d'autres solutions s'impose.

Investissement ciblé

Ce sont les nouvelles technologies qui motivent principalement la recherche et le changement de système d'exploitation. Cette observation confirme la tendance évoquée précédemment, les équipes de développement et d'administration modernes cherchent l'infrastructure la plus performante au lieu de s'en tenir à leurs outils internes habituels. Pour autant, les entreprises ne disposent pas de ressources illimitées et préfèrent dépenser le moins possible en prenant la bonne décision du premier coup. Le choix du système d'exploitation dépasse ainsi le cadre d'un simple serveur : il s'inscrit dans une plateforme globale, ce qui renforce l'importance de la décision d'investissement.

Ces investissements visent à répondre aux besoins métier. Les technologies évoluent et les entreprises doivent suivre le rythme. Par exemple, les entreprises prennent conscience que les fonctionnalités d'IA nécessitent une infrastructure et des outils de développement spécialisés que les systèmes d'exploitation standards ne prennent pas toujours en charge de manière adéquate. Certaines ont été contraintes de créer des fermes de serveurs massives basés sur des processeurs graphiques (GPU), dans le seul but de répondre aux besoins de leurs outils d'IA. Les entreprises les plus avancées intègrent cette accélération de l'innovation et adaptent leurs stratégies d'infrastructure pour en exploiter pleinement le potentiel. Leur objectif est d'évoluer assez rapidement pour bénéficier de la valeur

maximale des technologies, de manière maîtrisée, plutôt que de les déployer sans garantie de résultat.

Incertitude mondiale

L'incertitude mondiale s'est imposée comme un facteur déterminant dans la stratégie technologique des entreprises. Les tensions géopolitiques, à l'origine de préoccupations économiques, influencent aujourd'hui davantage les processus de décision que par le passé. Dans ce contexte, les entreprises ne peuvent plus évaluer leurs fournisseurs sous un angle strictement technologique : leurs choix doivent désormais être appréciés à l'aune de considérations géopolitiques. L'incertitude actuelle inquiète plus que jamais les entreprises[2], qui doivent tenir compte des droits de douane, des réglementations et des contrôles à l'exportation. Le caractère persistant et imprévisible de ces tensions géopolitiques fragilise les chaînes d'approvisionnement mondiales, ce qui pourrait conduire les entreprises à recentrer leurs écosystèmes technologiques à l'intérieur de leurs propres frontières.

Droits de douane et contrôle à l'exportation

Les préoccupations liées aux droits de douane, ainsi que les fluctuations monétaires potentielles qui en découlent, modifient la manière dont les entreprises envisagent les achats internationaux. Un contrat à long terme peut évoluer de manière significative un an après sa signature en cas de volatilité qui ferait varier les taux de change entre pays. C'est un enjeu majeur qui touche actuellement l'ensemble de la stratégie informatique. Depuis que cette dimension économique affecte le choix des fournisseurs, il n'est plus possible d'envisager un achat informatique comme autrefois.

Souveraineté numérique

Les pressions géopolitiques ne se limitent pas aux seuls enjeux économiques : les exigences réglementaires varient d'un pays à l'autre, modifiant la dynamique entre clients et fournisseurs. Ce phénomène est particulièrement visible dans le cloud computing, où des contraintes réglementaires telles que le Règlement général sur la

[2] McKinsey & Company, « Navigating the New Geopolitical Uncertainty », 16 janvier 2025, *https://www.mckinsey.com/capabilities/geopolitics/our-insights/navigating-the-new-geopolitical-uncertainty*

protection des données (RGPD) poussent les entreprises à privilégier des clouds « exclusivement européens » afin de garantir que les données restent hébergées au sein de l'Union européenne. Ce changement survient après des années de tensions, qui ont conduit de nombreuses entreprises à rechercher activement des fournisseurs cloud mieux adaptés à leurs exigences réglementaires spécifiques.

Incertitude économique

Les pressions économiques ont toujours eu un effet sur le monde de l'informatique. Combinée aux pressions mondiales, la rapidité des changements complique encore la situation. Les budgets disponibles sont limités, et les pénuries de compétences persistent : même lorsqu'il est possible de financer un poste d'administrateur supplémentaire, il peut s'avérer difficile de trouver le profil pour l'occuper.

En raison des contraintes budgétaires, l'optimisation des coûts est devenue un critère central dans la sélection du système d'exploitation Les entreprises accordent de plus en plus d'importance au ROI et à l'efficacité des dépenses. Ces nouvelles priorités ont des conséquences sur le choix du système d'exploitation, tant en matière d'investissement initial que de retour sur investissement.

Sécurité et fuites de données

La sécurisation des ressources informatiques est un enjeu majeur depuis de nombreuses années. Des études telles que 2025 Developer Survey de Stack Overflow montrent clairement que la sécurité, l'analyse des vulnérabilités et les tests figurent parmi les priorités des équipes de développement. Les inquiétudes liées à la sécurité et à la confidentialité arrivent en tête des raisons qui motivent l'abandon d'une technologie donnée.

Attaques de la chaîne d'approvisionnement

Il ne suffit pas de connaître l'origine des logiciels. Les entreprises doivent désormais également connaître la provenance des dépendances sur lesquelles ils reposent. Cette problématique représente en elle-même un risque de sécurité : si un composant mineur, mais essentiel à une solution logicielle majeure, est compromis, l'ensemble de l'entreprise est exposée. L'un des exemples les plus marquants reste la cyberattaque de 2021 visant SolarWinds, qui a exposé un grand nombre de ses clients à des violations de

données en raison de failles dans sa chaîne d'approvisionnement. Pourtant, le problème des dépendances demeure d'actualité. Récemment, le gestionnaire de paquets npm du registre JavaScript a été la cible d'une attaque de la chaîne d'approvisionnement qui a permis le déploiement de paquets censés être sûrs sur les appareils des utilisateurs dans le but d'y miner de la cryptomonnaie.

L'IA s'est révélée être à la fois un risque pour la sécurité et un levier de productivité et de performance opérationnelle. En très forte augmentation ces dernières années, les attaques basées sur l'IA ne semblent pas près de ralentir. Dans un rapport récent, l'agence d'évaluation de crédit Experian indique que l'IA est une menace suffisamment importante pour remplacer les erreurs humaines comme principale cause des fuites de données en 2026[3].

Préoccupations liées au chiffrement quantique

La menace émergente que représente l'informatique quantique fait l'objet de recherches depuis plusieurs années. La principale inquiétude réside dans le fait que, du fait de l'approche radicalement différente adoptée par les ordinateurs quantiques pour traiter les mécanismes de chiffrement classiques, l'ensemble des algorithmes de chiffrement actuels pourrait, à terme (probablement au cours des dix prochaines années, bien que ce calendrier fasse débat), être compromis en quelques secondes. Cette technologie rendrait vulnérables tous les fichiers et entrepôts de données chiffrés selon des méthodes classiques. Les pirates le savent et collectent d'ores et déjà autant de ressources que possible, même s'ils ne sont pas encore en mesure de les déchiffrer. Ce risque est désigné par l'expression « Harvest now, decrypt later », c'est-à-dire « Collecter aujourd'hui, déchiffrer plus tard ».

La cryptographie post-quantique fait référence à la nouvelle génération de méthodes de chiffrement conçues pour résister à la puissance des ordinateurs quantiques. Ce domaine est un axe de recherche récent en informatique. Tous les systèmes d'exploitation n'en tirent pas encore parti. L'utilisation de ces nouveaux algorithmes permet de déjouer les attaques de type « Harvest now, decrypt later ».

[3] Experian, « 2026 Data Breach Industry Forecast », 5 décembre 2025, *https://www.experian.com/thought-leadership/business/2026-data-breach-industry-forecast-report*

IA

L'IA s'est imposée comme un facteur dominant dans les décisions d'achat technologique. Établie depuis plusieurs années, cette tendance ne montre aucun signe de ralentissement. Fait notable, l'IA oriente de plus en plus le choix du système d'exploitation, tout comme les technologies qui lui sont associées.

Vibe coding

Avec l'IA, les cas d'utilisation modernes du système d'exploitation évoluent. La programmation, l'analyse de données et l'analyse métier sont désormais accessibles aux profils qui n'ont pas de formation technique ou spécialisée. À titre d'exemple, le vibe coding désigne une méthode de création d'applications assistée par l'IA qui ne requiert pas de formation spécialisée en programmation ou développement. Le marché tend ainsi à privilégier les systèmes d'exploitation compatibles avec les outils de développement assistés par l'IA, capables de favoriser ce type de pratiques.

Accélération matérielle

Par ailleurs, il existe encore des cas d'utilisation traditionnels de l'IA qui nécessitent un système d'exploitation puissant. Pour certaines tâches, telles que l'inférence, l'entraînement des modèles ou l'hébergement d'un dialogueur basé sur un LLM, le système d'exploitation doit interagir efficacement avec les GPU et les autres ressources matérielles personnalisées. Quand des puces spécialisées permettent d'accroître les performances, l'échelle et la flexibilité des fonctionnalités d'IA, la compatibilité matérielle devient un critère de sélection déterminant. Les fonctions d'automatisation et de gestion basées sur l'IA continueront de solliciter fortement les ressources matérielles disponibles. Par conséquent, la capacité d'un système d'exploitation à exploiter des architectures matérielles avancées influence directement son choix.

Conclusion

Les bouleversements du marché qui incitent les entreprises à réévaluer leurs choix de systèmes d'exploitation représentent une opportunité stratégique d'explorer de nouvelles perspectives. Elles prennent conscience des possibilités sans précédent créées par cette combinaison

d'instabilité mondiale et d'accélération de l'innovation. Elles adoptent une posture de plus en plus proactive, en explorant de nouvelles options au lieu de s'en tenir à des plateformes existantes qui ne suivent plus nécessairement le rythme des changements. Autrefois considéré comme une contrainte, le choix du système d'exploitation est devenu un facteur majeur d'amélioration de l'exploitation métier. L'enjeu est d'identifier la solution la plus adaptée dans un contexte de mutation rapide, plutôt que de perpétuer des pratiques héritées du passé.

CHAPITRE 2

Des problèmes aux solutions

Dans le chapitre 1, nous avons identifié des facteurs importants dans le choix d'un système d'exploitation : l'accélération de l'innovation, l'incertitude mondiale, les pressions économiques, les enjeux de sécurité et les exigences relatives à l'IA. Ce n'est toutefois qu'un début. Le véritable défi pour les responsables informatiques consiste à gérer ces pressions de manière efficace, sans introduire de nouvelles sources de complexité ni de vulnérabilités. Pour réussir, il faut reconnaître ces problèmes et y réagir de manière productive et compétitive. Dans ce chapitre, nous allons examiner chacun de ces défis et proposer des solutions pour les relever.

Stratégies d'accélération de l'innovation

Pour les responsables informatiques, l'accélération de l'innovation est devenue une force motrice. Au-delà de la simple nécessité de suivre la concurrence, des notions telles que l'avantage du pionnier montrent que les entreprises capables d'agir rapidement captent souvent la plus grande part de valeur. Cette dynamique a une forte influence sur le choix du système d'exploitation, car ce dernier sert de base sur laquelle repose l'innovation que l'entreprise cherche à exploiter. Ce type d'innovation conduit les entreprises vers des territoires encore peu explorés, ce qui impose une approche mesurée, fondée sur des besoins clairement identifiés et des bénéfices tangibles. L'improvisation n'a pas sa place dans l'accélération de l'innovation. Un système d'exploitation moderne doit favoriser l'expérimentation tout en assurant la sécurité, les performances et la fiabilité.

Expérimentation rapide et maîtrisée

Avec l'accélération de l'innovation technologique, les méthodes de développement et d'évaluation traditionnelles ne sont plus assez rapides. Dans le domaine du développement d'applications, cette évolution est déjà bien établie : les cycles de lancement annuels basés sur des approches en cascade ont laissé place au développement agile, puis à la distribution continue portée par le DevOps, jusqu'aux modèles actuels de déploiement ultrarapides avec plusieurs mises à jour quotidiennes. Cette tendance s'étend désormais à tout le paysage technologique et les responsables informatiques ont compris qu'ils doivent s'y conformer pour garder une longueur d'avance.

Ce rythme d'innovation nécessite des cycles rapides de développement et de test, ainsi que le maintien d'un socle de sécurité qui empêche les entreprises de s'exposer aux risques. Une expérimentation efficace repose sur des environnements de type sandbox avancés, capables de reproduire des conditions proches de la production sans mettre en danger les données de l'entreprise ni le système d'exploitation qui héberge les applications. Il s'agit du moyen le plus efficace d'obtenir des environnements de test réalistes qui permettent d'évaluer rapidement les performances dans des conditions de production réelle.

Dans la même logique, les applications doivent pouvoir passer de manière fiable et rapide d'une étape à l'autre. Ce processus doit être transparent, afin que les applications validées en environnement de test puissent être déployées en production avec un haut niveau de fiabilité. Au-delà de la simplicité d'usage, la reproductibilité et la fiabilité garantissent que les mises à jour sont aussi efficaces et sûres que les déploiements initiaux.

Dans ce contexte, il est clairement bénéfique d'adopter une approche ouverte et mesurée dans le choix du système d'exploitation. L'agilité à l'ère de l'innovation accélérée représente un avantage stratégique réel. Puisque le système d'exploitation héberge les applications et que les exigences de celles-ci évoluent rapidement, les entreprises doivent s'assurer que leur système est en mesure de suivre ce rythme. Cette approche nuancée est confirmée par les analyses d'acteurs tels que IDC et McKinsey. En juin 2024, McKinsey a déclaré qu'en vérité, il n'existait pas d'approche universelle, mais que les entreprises

pouvaient aligner leurs objectifs d'innovation avec la nécessité de maintenir des infrastructures technologiques robustes et fiables[1].

Pour autant, il convient de sélectionner les outils et les technologies avec soin. Tout changement doit remplir un objectif précis et apporter un avantage afin de justifier l'augmentation de la complexité qu'il entraîne, en particulier pour un élément aussi essentiel que le système d'exploitation. Les décisions doivent s'appuyer sur des éléments probants démontrant des gains réels en matière de capacités organisationnelles. Ces bénéfices doivent être mesurables. La nouveauté seule ne justifie pas l'adoption d'un nouveau système. Ainsi, les entreprises doivent évaluer non seulement les fonctionnalités actuelles d'un système d'exploitation, mais également à sa stabilité et son potentiel d'évolution.

Architecture axée sur la sécurité

Les entreprises ne sont pas les seules à bénéficier de la rapidité de l'innovation technologique. Les menaces de cybersécurité continuent d'évoluer, exposant aux attaques les entreprises qui ne protègent pas assez leur environnement. Des études de marché, telles que le *rapport Global Threat Rapport 2025* de CrowdStrike, montrent clairement que les cybermenaces progressent toujours plus rapidement que les mécanismes de défense. Les menaces modernes présentent des défis inédits et en constante évolution que de nombreux outils et cadres de sécurité traditionnels ne sont pas capables de relever. La préparation à ces risques est devenue un impératif stratégique.

La sécurité doit être pleinement intégrée lors de la mise en œuvre d'un nouveau système d'exploitation. Les entreprises qui négligent les enjeux de sécurité et les processus de vérification dans leur démarche de sélection s'exposent à un double risque, au niveau des applications hébergées sur le système, ainsi qu'au niveau de la sécurité et de la fiabilité du système lui-même. Ce constat est d'autant plus pertinent aujourd'hui que les fournisseurs intègrent de plus en plus de fonctions d'IA à leurs produits, leur conférant un niveau d'accès élevé pour automatiser des tâches d'administration système.

[1] McKinsey, « Rethinking Conventional Wisdom: Future of Digital Tech Infrastructure », 26 juin 2024, *https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/tech-forward/rethinking-conventional-wisdom-future-of-digital-tech-infrastructure*

La sécurité des données, un impératif

Le système d'exploitation doit offrir des environnements qui assurent la sécurité des applications et du stockage des données. Les entreprises doivent pouvoir garantir que tout ce qui s'y exécute (des composants natifs aux applications hébergées) reste protégé. Voici les trois catégories de données à sécuriser :

Données au repos
: Il s'agit des données stockées en vue d'une utilisation ultérieure.

Données en transit
: Ces données sont échangées d'une application à une autre, que ce soit entre plusieurs systèmes ou au sein d'un même système.

Données en cours d'utilisation
: Ces données sont activement traitées par la plateforme de calcul.

Le chiffrement permet souvent de sécuriser les données au repos et en transit. En revanche, la protection des données en cours d'utilisation s'avère plus complexe. Les architectures modernes de systèmes d'exploitation résolvent ce problème en intégrant un environnement d'exécution de confiance, ou TEE (Trusted Execution Environment). Il s'agit d'un espace du système réservé à des logiciels hautement fiables et accessible uniquement par le biais de mécanismes strictement contrôlés. Tout ce qui s'exécute dans un environnement TEE n'est généralement pas accessible depuis l'extérieur. Cette solution, qui peut s'appuyer sur des composants matériels et logiciels, couvre souvent plus d'un serveur et nécessite l'actualisation constante des pilotes et de la compatibilité afin de conserver toutes ses fonctionnalités. Les modalités de mise en œuvre varient en fonction des fournisseurs et n'entrent pas dans le cadre de ce rapport. Cependant, il est essentiel pour les entreprises de vérifier que leurs applications peuvent d'exécuter dans de tels environnements sécurisés.

Le cas particulier des charges de travail d'IA

Nous venons d'établir que la protection et la souveraineté des données étaient nécessaires pour toutes les charges de travail de calcul. Toutefois, les charges de travail d'IA sont particulièrement vulnérables en raison de leur caractère récent, de leur forte consommation de données et de leur complexité algorithmique.

Leur nouveauté implique que les charges de travail de production n'ont pas encore bénéficié du même niveau de test et de maturité que les charges de travail traditionnelles. La sécurité est le fruit d'un travail collaboratif, et l'ensemble des acteurs du marché effectue bien plus de tests et de contrôles qualité que tout fournisseur isolé, tant pour le produit lui-même que pour sa configuration ou son utilisation. Dans son rapport *Cloud Security Risk Report 2025*, Tenable indique que les charges de travail cloud compatibles avec l'IA sont plus vulnérables que les autres. Quel que soit l'environnement d'hébergement des charges de travail, le volume élevé de données que consomme l'IA ainsi que les erreurs de configuration et les vulnérabilités persistantes imposent un niveau de précaution accru en matière de cybersécurité.

Les entreprises doivent prendre en compte les risques liés à l'IA lorsqu'elles évaluent un système d'exploitation. À défaut, elles s'exposent à un niveau de risque difficile à maîtriser, susceptible de compromettre les charges de travail actuelles comme futures.

Conclusion

Pour faire un choix éclairé, les entreprises doivent repenser la manière dont elles évaluent les technologies. Les défis présentés dans ce chapitre guident le processus de sélection en vue de maximiser l'avantage concurrentiel. À la fin de ce rapport, nous proposerons un cadre décisionnel qui intègre l'ensemble de ces dimensions. À ce stade, il paraît évident que le déploiement du système d'exploitation doit être repensé : les défis modernes appellent des solutions modernes. Les entreprises qui relèvent ce défi avec une vision stratégique se positionnent favorablement pour tirer parti des nouvelles technologies et asseoir leur avantage concurrentiel.

CHAPITRE 3

La plateforme Linux moderne

L'exploitation des serveurs sous Linux s'est généralisée dans les entreprises modernes. De nombreuses études ont confirmé cette tendance au cours des dix dernières années. Par exemple, en août 2025, SQ Magazine a révélé que 61,4 % des grandes entreprises exécutaient au moins une charge de travail essentielle sur un système Linux et que 78,3 % des serveurs web connectés à Internet fonctionnaient sous Linux[1]. Cette position dominante est le résultat de plusieurs années de croissance, une dynamique qui ne montre aucun signe de ralentissement.

Toutefois, ces études ne distinguent pas souvent les différentes distributions, ce qui conduit certains décideurs à considérer que tous les systèmes Linux se valent. C'est inexact. Certes, toutes les distributions Linux reposent sur le même noyau, mais les modalités de déploiement de ce noyau ainsi que l'écosystème d'outils et d'applications qui l'entoure peuvent varier de manière significative.

Les entreprises doivent donc identifier les facteurs qui différencient les systèmes d'exploitation qu'elles évaluent. De nombreux systèmes modernes proposent des fonctions de pointe, mais celles-ci ne sont pas toujours mises en œuvre de la même façon ni disponibles partout. Parmi les critères les plus intéressants figurent les modèles de déploiement modernes et sécurisés, les outils système intégrant l'IA, les outils de gestion de l'environnement, les mécanismes de sécurité d'entreprise, ainsi que l'étendue de la prise en charge et des

[1] Robert A. Lee, « Linux Statistics 2025: Desktop, Server, Cloud & Community Trends », *SQ Magazine*, dernière mise à jour le 18 novembre 2025, *https://sqmagazine.co.uk/linux-statistics*

certifications de partenaires. En outre, les fonctionnalités offertes par un système d'exploitation doivent être évaluées au regard des exigences des charges de travail qu'il est destiné à héberger, en privilégiant des fonctions de pointe adaptées aux besoins actuels.

Le déploiement de système d'exploitation repensé

Les méthodes de déploiement des systèmes d'exploitation n'ont pas beaucoup changé au fil des ans. Le déploiement traditionnel reposait sur un programme d'installation chargé de déployer le noyau et les outils associés sur le disque, puis sur l'installation des applications par les utilisateurs. L'apparition de la gestion de paquets a considérablement facilité la gestion des applications et l'administration des systèmes, car les utilisateurs n'avaient plus à compiler du code à partir de zéro à chaque installation ou mise à jour.

Une distribution Linux moderne doit fournir un mode de déploiement où les systèmes prennent la forme de conteneurs immuables qui peuvent être remplacés selon les besoins. Il suffit alors de télécharger une nouvelle image et de redémarrer le système pour effectuer la mise à niveau (ou la restauration d'une version antérieure) du composant modifié. Cette approche garantit la sécurité et la fiabilité, et permet de s'assurer que l'ensemble de l'environnement exécute les versions attendues de tous les fichiers binaires et de toutes les bibliothèques.

Les images ainsi créées peuvent être gérées de la même manière que les conteneurs (ou images) d'applications, mais à une échelle encore plus petite (au niveau des fichiers binaires, voire du noyau du système d'exploitation). Il s'agit d'une amélioration majeure par rapport à l'ancien modèle de mise à jour basé sur les paquets. Même si ces derniers sont plus efficaces que la compilation à partir du code source, ils présentent des problèmes spécifiques en matière de compatibilité, d'exigences et de conflits de versions. Un modèle basé sur les conteneurs élimine ces problèmes, car tous les éléments se trouvent dans l'image. Les versions de tous ces composants restent cohérentes, ce qui réduit fortement les risques d'écart de configuration. De plus, l'installation d'une image est beaucoup plus simple et rapide : il suffit de la télécharger, de l'appliquer et de redémarrer le système.

Parce qu'elles sont immuables, les images renforcent également la sécurité. Un pirate ou un logiciel malveillant ne pourrait pas modifier l'image en place ni la remplacer. Puisque ces images sont gérées de la même manière que les conteneurs d'applications, il est possible de les examiner avec un outil de conteneurisation standard, comme Podman, ou de nombreuses autres plateformes de conteneurs courantes. Ainsi, les administrateurs qui maîtrisent déjà les conteneurs d'applications peuvent déployer des images de système d'exploitation rapidement et en toute confiance.

Enfin, les images créées peuvent être utilisées dans tous les environnements : cloud, physiques, virtualisés ou à la périphérie du réseau. Elles sont déployées et exécutées de la même manière partout, et leur gestion est simplifiée du début à la fin. La figure 3-1 montre un exemple de processus en mode image structuré en trois étapes simples : la création d'images, le déploiement et la gestion.

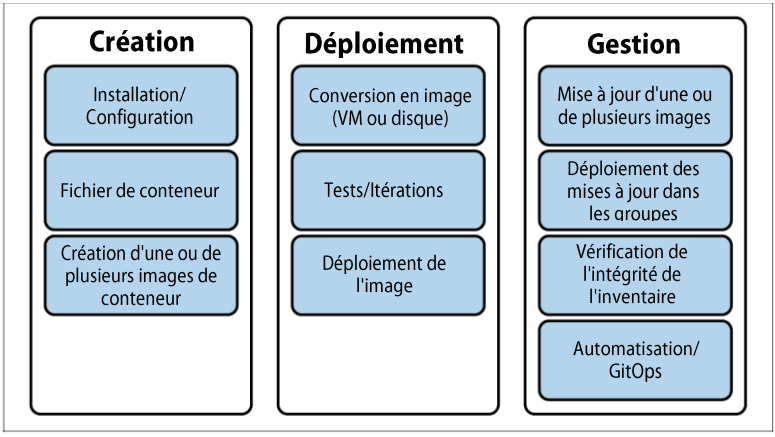

Figure 3-1 : exemple d'un modèle de déploiement de système d'exploitation conteneurisé (en mode image)

Administration système assistée par l'IA

Dans le domaine du développement d'applications, il devient courant d'intégrer l'IA directement aux outils d'administration système, tels que les émulateurs de terminal (qui permettent d'accéder à la ligne de commande). Très utiles, ceux-ci offrent aux équipes d'administration la possibilité d'interroger les LLM de leur choix sans ouvrir de fenêtre de navigateur ni d'application distincte. C'est à présent au tour des

fournisseurs de systèmes d'exploitation d'intégrer l'IA directement au système d'exploitation. L'assistant IA deviendrait alors accessible à partir de la ligne de commande, quel que soit le terminal choisi par l'utilisateur. Cette fonctionnalité serait d'une grande aide aux administrateurs de tous les niveaux et tout particulièrement aux profils débutants qui pourraient interroger directement un assistant d'IA en ligne de commande afin de valider leurs actions en temps réel et s'assurer qu'ils ne font pas d'erreurs.

Comme tous les outils d'IA, les assistants en ligne de commande doivent être utilisés avec précaution. L'obtention de réponses précises peut nécessiter d'affiner les requêtes, en particulier lorsque l'assistant est sollicité pour générer du code, par exemple des scripts shell.

En cas de doute, il est recommandé aux débutants de demander à un collègue plus expérimenté si les réponses données par l'assistant d'IA produiront bien les résultats attendus.

Cet outil ne se limiterait pas à comprendre des scripts bash de base. Les assistants en ligne de commande pourraient offrir des conseils pratiques sur la configuration des applications et des services, ainsi que sur l'utilisation des fonctions du système d'exploitation pour résoudre les problèmes. L'entraînement de ces assistants couvrirait non seulement Linux en général, mais aussi les subtilités et les exigences spécifiques de la distribution utilisée. Ce processus de réglage fin est bien connu dans le domaine de l'IA. L'utilisation d'un modèle personnalisé, plutôt qu'un modèle généraliste, entraîné uniquement sur de la documentation pertinente et conçu pour réduire les hallucinations, fait de ce type d'outil un atout concurrentiel plus important quand il est intégré directement dans le système.

Un assistant en ligne de commande peut s'avérer particulièrement utile pour des outils tels que SELinux (Security-Enhanced Linux) et le pare-feu intégré. Bien qu'essentiels au fonctionnement du système, ces deux éléments sont complexes et leurs configurations ne sont modifiées qu'occasionnellement, dans la plupart des cas. Or, la configuration de ces outils devient beaucoup plus rapide et plus facile avec un assistant en ligne de commande. En s'appuyant sur un large ensemble d'exemples validés, l'outil est également en mesure d'identifier des erreurs de configuration qui pourraient passer inaperçues, même pour des administrateurs expérimentés.

Enfin, les assistants en ligne de commande facilitent la compréhension de la structure des outils utilisés. Ils peuvent par exemple expliquer comment sont mis en œuvre les pare-feux modernes basés sur des hôtes. Ils interrogent les ressources pertinentes à la recherche des meilleures pratiques et d'exemples basés sur la demande formulée, puis génèrent une réponse en langage naturel qui complète les modifications à apporter à la configuration ou au code source en explicitant les recommandations formulées.

Outils de gestion de l'environnement

Les deux puissants outils que nous avons évoqués simplifient considérablement la gestion des systèmes à l'échelle individuelle. Pour aller plus loin, il faudrait un autre outil qui favorise une gestion proactive de l'ensemble de l'environnement Linux déployé. Un tel outil proposerait des intégrations étroites avec tous les composants de l'offre du fournisseur de système d'exploitation, permettant ainsi de gérer toute la plateforme à partir d'un seul endroit et de simplifier la gestion ainsi que les audits. Idéalement, il inclurait une fonction de planification qui facilite la compréhension du cycle de vie des applications déployées et leurs effets sur les systèmes qui s'exécutent dans l'environnement. Grâce à ces intégrations, il serait possible d'effectuer des validations de sécurité et de configuration en temps réel dans toute l'entreprise.

Les fonctions de feuille de route fourniraient des informations détaillées sur les futures applications et versions du système d'exploitation. Les entreprises pourraient ainsi planifier les mises à niveau selon les nouvelles fonctions à venir, au lieu de réagir après leur lancement.

Les outils de gestion de l'environnement peuvent également servir à maintenir les systèmes à jour. La gestion coordonnée des correctifs (automatisée ou planifiée et confirmée), les mises à jour ou déploiements de fonctions et de logiciels, ainsi que la gestion centralisée des configurations simplifient la gestion des serveurs, même lorsqu'il y en a plus d'un millier.

Sécurité adaptée aux entreprises

Un système d'exploitation véritablement axé sur la sécurité ne se limite pas aux mécanismes mentionnés précédemment (images immuables, gestion de la configuration, etc.).

Les attaques par cryptographie post-quantique est une grande source de préoccupation pour l'avenir. Nous avons vu dans un chapitre précédent que cette technologie fournit aux entreprises des algorithmes résistant aux attaques quantiques pour les clés, le chiffrement et les signatures numériques. Elle contribue à pérenniser la sécurité des données et des applications et représente un critère essentiel dans l'évaluation des distributions de systèmes d'exploitation.

Un système d'exploitation d'entreprise doit également offrir un ensemble robuste de fonctions de sécurité pour la chaîne d'approvisionnement. Cette approche dépasse le seul système d'exploitation : elle s'inscrit dans une logique de plateforme qui vise à accompagner les équipes de développement et les entreprises adoptant des pratiques DevSecOps. Un exemple simple consiste à proposer un emplacement de confiance pour l'hébergement de dépendances d'applications validées. Il est toutefois possible d'aller encore plus loin. Une plateforme DevSecOps idéale devrait fournir aux équipes de développement un pipeline de sécurité de bout en bout pour toutes les applications et dépendances.

Ensemble, les mesures de protection par cryptographie post-quantique, les outils de sécurité automatisés pour les équipes d'administration et de développement ainsi que les systèmes de gestion proactive des logiciels forment une défense multicouche évolutive pour faire face aux menaces sophistiquées d'aujourd'hui. Ces mécanismes de sécurité sont directement intégrés aux outils et au système d'exploitation qu'utilise l'entreprise. Cette stratégie offre une plateforme complète qui évite un recours systématique à des solutions de sécurité tierces externes.

Extension du support matériel et logiciel et certification

Aussi performante soit-elle, une plateforme de système d'exploitation ne fonctionne pas toute seule. Elle doit être compatible avec le

matériel sur lequel le système d'exploitation s'exécute ainsi qu'avec les logiciels tiers qui y seront utilisés.

À l'heure actuelle, le marché de la compatibilité matérielle évolue rapidement. Les équipements utilisés pour l'IA connaissent notamment une progression fulgurante que les pilotes de système d'exploitation et les mécanismes de compatibilité doivent suivre. La distribution sélectionnée doit se distinguer sur ce point, en fournissant des bibliothèques d'IA, des pilotes et des applications à jour, ainsi que des optimisations matérielles pour des fournisseurs comme NVIDIA, Intel et AMD. Au-delà de ces trois acteurs majeurs, un éditeur de systèmes d'exploitation doit aussi s'appuyer sur un écosystème tiers robuste, capable de fournir rapidement, de manière sécurisée et fiable, les dernières fonctions aux utilisateurs.

Conclusion

Les mesures de sécurité, l'écosystème et les fonctions d'un système d'exploitation contribuent conjointement à répondre à l'impératif stratégique identifié au début de ce rapport, à savoir, l'exploration d'autres systèmes d'exploitation. Les principales fonctions présentées dans ce chapitre permettent de distinguer les systèmes d'exploitation, tant sur le plan des capacités que de la facilité de gestion. Le choix d'une nouvelle plateforme doit s'appuyer à la fois sur les avancées technologiques et sur la solidité des programmes de partenariat.

CHAPITRE 4

Étapes suivantes

Pour les entreprises, le choix du système d'exploitation représente un enjeu majeur qui affecte la position concurrentielle et la gestion de l'infrastructure interne. Il leur faut une plateforme spécialement conçue pour gérer la pression liée à l'accélération de l'innovation, à l'incertitude mondiale, aux contraintes économiques, aux besoins modernes en matière de sécurité et à l'IA, le tout de manière intégrée.

Ce n'est pas une décision à prendre à la légère. Voici les quatre grandes étapes à suivre pour choisir les systèmes d'exploitation et plateformes à mettre en place :

- Identifier les enjeux les plus importants pour l'entreprise
- Mettre en corrélation les charges de travail et les fonctionnalités requises
- Évaluer la valeur globale pour l'entreprise
- Valider la sécurité de la chaîne d'approvisionnement et la viabilité de la solution à long terme

Identifier les enjeux les plus importants

Il faut savoir que les enjeux varient selon les équipes. Celles chargées des produits d'IA accordent la priorité à l'innovation et aux exigences matérielles, tandis que dans les secteurs réglementés, l'accent est mis sur les fonctionnalités de sécurité et de conformité. Les entreprises doivent évaluer chaque domaine de pression (accélération de l'innovation, incertitude mondiale, contraintes économiques, exigences de sécurité et IA) en fonction de leur importance actuelle et

future, puis s'appuyer sur cette analyse pour distinguer les critères indispensables des éléments secondaires dans leurs évaluations.

Mettre en corrélation les charges de travail et les fonctionnalités requises

Les charges de travail les plus stratégiques pour une entreprise représentent un facteur déterminant dans la définition des exigences. En les analysant, il est possible de déterminer s'il vaut mieux opter pour une optimisation spécifique par charge de travail ou pour une approche de standardisation plus large. Cette démarche s'applique à toutes les entreprises, indépendamment de leur taille, puisque le nombre et l'importance des charges de travail ne sont pas nécessairement corrélés à celle-ci.

Évaluer la valeur métier

Une fois les charges de travail analysées, l'entreprise dispose d'une vision précise du nombre de serveurs, des effectifs (et de leur niveau de compétence) ainsi que du volume global de charges de travail à gérer. Elle peut ainsi évaluer les coûts directs, tels que les licences du système d'exploitation, l'assistance et les besoins en matière d'infrastructure. Elle peut également estimer les coûts indirects, comme le niveau d'expertise interne, les retards de déploiement des charges de travail dus à des contraintes imprévues ainsi que les opportunités commerciales manquées en raison du manque de flexibilité de l'infrastructure. Ces données permettent de prendre des décisions stratégiques plus éclairées afin d'améliorer l'efficacité opérationnelle et de renforcer l'avantage concurrentiel.

Valider la sécurité de la chaîne d'approvisionnement et la viabilité de la solution à long terme

Lors du choix d'un système d'exploitation ou d'une plateforme, il est essentiel de s'assurer de sa viabilité à long terme En plus d'examiner l'historique d'un fournisseur, les entreprises doivent également évaluer ses processus de validation des applications, la richesse de son

écosystème de partenaires, ainsi que ses capacités en matière de conformité réglementaire et d'intégration de fonctions avancées telles que l'IA. Les déploiements de charges de travail ont généralement un cycle de vie de plusieurs années. Il faut donc absolument s'assurer que la plateforme sélectionnée est en mesure de les gérer à long terme.

Conclusion

Le plus important est de comprendre que les décisions liées à l'infrastructure créent des dépendances. Les choix d'aujourd'hui peuvent soit favoriser la réussite de l'entreprise, soit limiter les capacités et retarder les projets pendant des années. Les entreprises qui abordent la sélection du système d'exploitation de manière stratégique, en s'appuyant sur des exigences clairement définies et un cadre d'évaluation structuré, se donnent les moyens d'accélérer l'innovation, de gérer efficacement l'incertitude et d'optimiser à la fois leur productivité et leur sécurité, aujourd'hui comme demain.

À propos des auteurs

Ned Bellavance est un professionnel de l'informatique et un instructeur technique qui dispose de plus de 20 ans d'expérience dans le domaine. Il a travaillé comme opérateur de service d'assistance, administrateur système, architecte cloud et responsable produit. Il a récemment lancé son entreprise Ned in the Cloud LLC, avec laquelle il développe des cours, anime plusieurs podcasts, écrit des livres et crée des contenus originaux pour les fournisseurs de technologies. Ned Bellavance est reconnu comme expert par Microsoft depuis 2017, et comme ambassadeur par HashiCorp depuis 2020. Il suit trois principes clés : accepter l'inconfort, se préparer à l'échec et faire preuve de bienveillance.

Chris Hayner est un professionnel de l'informatique expérimenté qui travaille avec les systèmes d'exploitation, les infrastructures, le cloud computing et la cybersécurité depuis plusieurs dizaines d'années. Sa carrière a commencé dans un datacenter où il gérait différents systèmes, dont des mainframes, des AlphaServers et des serveurs x86 générique. Il a ensuite étendu son champ d'action à la virtualisation, aux technologies cloud et aux stratégies informatiques et de cybersécurité globales. Ces 15 dernières années, il a travaillé dans le domaine du consulting comme spécialiste, architecte et analyste. À ce titre, il a aidé des centaines d'entreprises à choisir les bonnes solutions informatiques pour leurs objectifs métier, stimulant ainsi l'innovation et la réussite. En plus de nombreuses certifications professionnelles, dont le CISSP, Chris Hayner a obtenu son MBA à l'université Temple, ce qui lui permet d'appréhender à la fois les aspects techniques et métier du secteur.