



IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

L'évolution des exigences de la DEX (Gestion de l'expérience numérique)

eBook EMA, juillet 2022
par Steve Brasen

Réalisé pour

ivanti



Table des matières

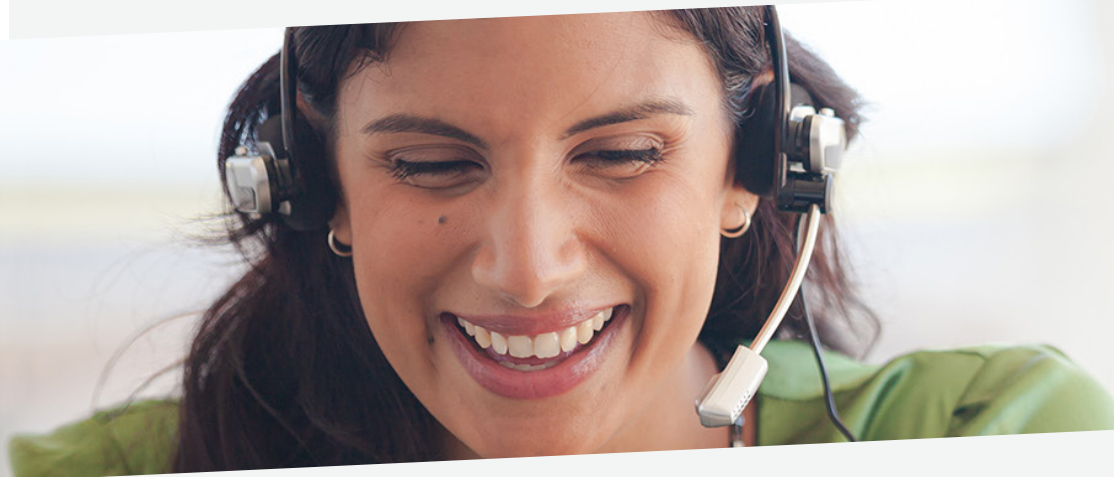
- 1** L'adoption d'une théorie de management moderne
- 2** Les obstacles à l'expérience numérique
- 3** L'expérience collaborateur dans un monde multi-périphériques
- 4** Comment prendre en charge l'Everywhere Workplace
- 5** L'impact de la sécurité sur l'expérience collaborateur
- 6** Les critères d'identification d'une solution performante

L'adoption d'une théorie de management moderne

Ces dernières années, les entreprises ont repensé leurs systèmes et adopté une approche de l'IT centrée sur l'utilisateur. En particulier, la « théorie du management moderne » part du postulat que la satisfaction au travail contribue à une hausse de la productivité de la main-d'œuvre. Si l'on applique ce principe à l'époque actuelle, l'utilisation de l'IT impose que la technologie numérique soit au service des collaborateurs, et non l'inverse.

Aujourd'hui, le type et l'usabilité des technologies fournies par l'entreprise aux collaborateurs sont les principaux facteurs d'attraction et de rétention des talents. D'après une étude menée par Ivanti, fournisseur de solutions de gestion IT, 41 % des entreprises interrogées disent avoir perdu du personnel IT du fait d'une charge de travail excessive. Au lieu de se concentrer sur la mise en place d'une technologie « centrée sur l'utilisateur » dont le seul but est de rendre les employés productifs,¹ les approches de management modernes sont axées sur l'optimisation de l'expérience collaborateur pour améliorer à la fois la productivité et la satisfaction au travail.

De plus en plus, les entreprises fixent des exigences spécifiques d'amélioration de l'expérience collaborateur via la transformation digitale et des outils de management modernes. Ces objectifs sont ajoutés aux SLA (accords de niveau de service) existants ou documentés séparément dans des XLA (accords de qualité d'expérience). Les tendances émergentes en matière de gestion IT montrent clairement que les entreprises se concentrent sur l'amélioration de l'expérience numérique des collaborateurs pour relever les principaux défis technologiques du moment.



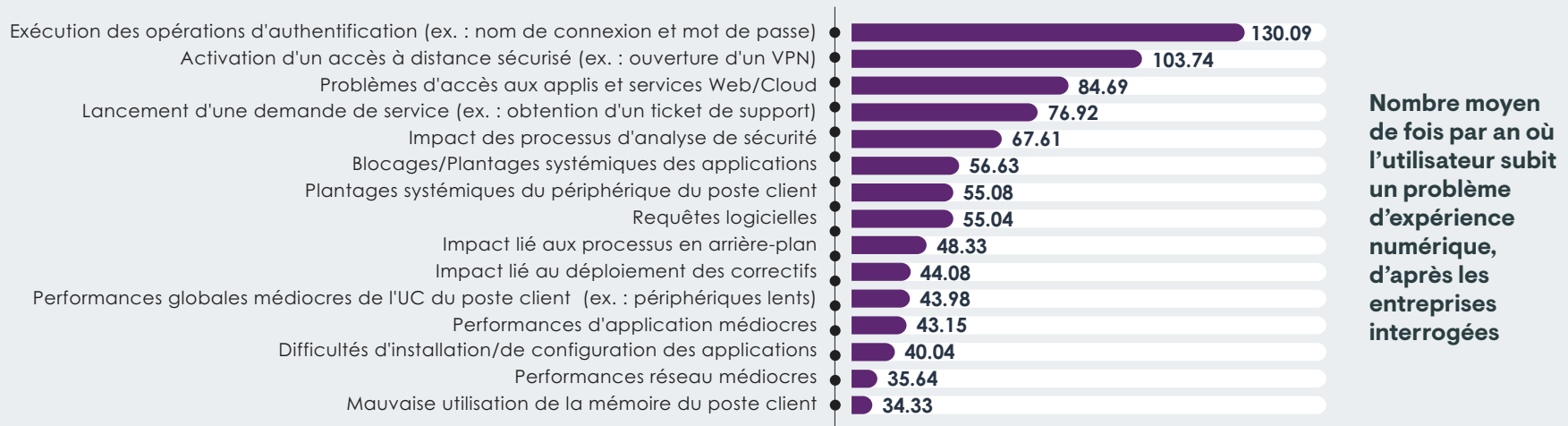
¹ « Top IT Trends for the Everywhere Workplace », 2021

Les obstacles à l'expérience numérique

On mesure facilement l'importance de la gestion de l'expérience numérique des collaborateurs en évaluant simplement le nombre des événements qui impactent leur productivité. En moyenne, les collaborateurs qui utilisent régulièrement la technologie numérique pour leur travail sont affectés par un problème de gestion des terminaux 919 fois par an, soit environ 3,67 problèmes par jour ouvrable.² Et chacun de ces problèmes peut avoir un effet boule de neige sur les performances des collaborateurs. Chaque fois qu'un utilisateur est distrait de l'exécution d'une tâche professionnelle, il lui faut jusqu'à 20 minutes pour se recentrer sur son travail une fois le problème résolu.

La fréquence de cet impact sur l'expérience collaborateur nuit également à l'efficacité des administrateurs IT. En moyenne, 40 % des collaborateurs d'une entreprise contactent le centre de support chaque semaine pour un problème d'expérience numérique, surchargeant inutilement le personnel de support et augmentant le coût global des opérations IT. Pire encore, beaucoup de travailleurs renoncent à contacter le service de support et demandent plutôt à un homologue non qualifié une solution de contournement qui, en réalité, peut encore réduire sa productivité. Dans ce cas, la cause première de la perturbation n'est jamais découverte et les incidents sont voués à se répéter jusqu'à ce que le problème soit signalé à un administrateur IT.

Le personnel d'une entreprise peut subir une très grande variété de problèmes ayant des effets préjudiciables sur la productivité. Cependant, les plus fréquents sont liés au respect des exigences de sécurité, comme l'authentification d'accès, l'établissement de connexions VPN, l'analyse antimalware et les déploiements de correctifs. On rencontre aussi fréquemment des difficultés d'accès aux services SaaS et Web dans le Cloud.



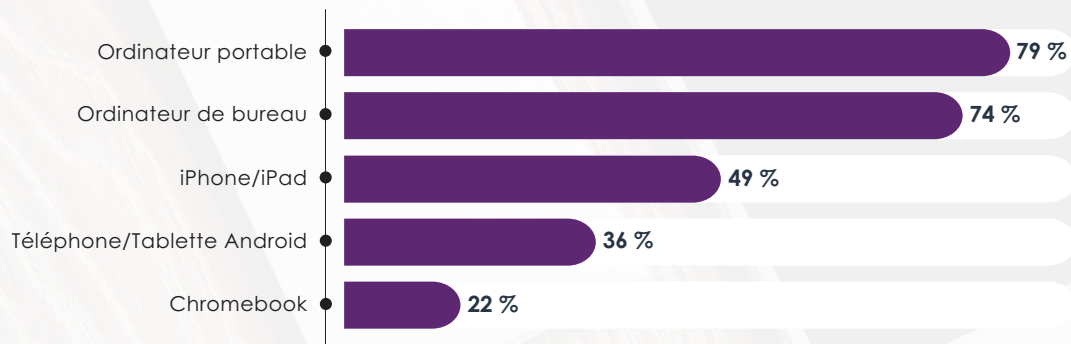
² « Identifying Effective Digital Employee Experience (DEX) Management Solutions: A Quantitative Analysis », 2021

L'expérience collaborateur dans un monde multi-périphériques

Les collaborateurs qui s'appuient sur la technologie numérique pour travailler utilisent aujourd'hui (en moyenne) 2,6 périphériques différents, notamment des PC de bureau, des ordinateurs portables, des smartphones et des tablettes.³ Pour être productifs, ils doivent pouvoir accéder aux ressources IT de l'entreprise et les utiliser de manière cohérente sur tous les périphériques, quelle que soit leur fréquence d'utilisation. Cependant, la garantie d'une expérience transparente peut s'avérer difficile, étant donné que le format unique de chaque périphérique (taille d'écran, périphériques d'entrée, système d'exploitation, etc.) nécessite des interactions utilisateur différentes.

Les méthodes employées pour obtenir et utiliser les différentes applications et services IT varient aussi énormément selon le type de périphérique. Certains utilisateurs téléchargent des ressources via des App Stores ou des portails d'applis d'entreprise, tandis que d'autres utilisent des applis SaaS, Web ou virtuelles. Enfin, les types et les configurations des périphériques doivent s'adapter aux préférences de chaque utilisateur.

Pourcentage de personnes interrogées indiquant utiliser les types de périphériques suivants pour travailler



La grande variété des configurations de poste client rend difficile la mise en place d'une gestion cohérente et centralisée de l'expérience utilisateur sur tous les périphériques des collaborateurs. En général, c'est parce que les administrateurs manquent de visibilité globale sur l'ensemble des périphériques, ce qui les empêche de corriger l'état des périphériques et les activités des utilisateurs.

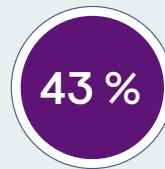
Pour évaluer correctement l'expérience des utilisateurs, les entreprises doivent identifier et corriger tous les problèmes et dégradations de performances, et détecter les opportunités d'amélioration de façon cohérente sur l'ensemble des périphériques en temps réel. Les fonctions de gestion unifiée des terminaux (UEM), qui incluent une prise en charge multiplateforme solide gérée de façon centralisée, améliorent sensiblement les solutions DEX.

³ « EMA Contextual Awareness Research Report », 2020

Comment prendre en charge l'Everywhere Workplace

Pour répondre à la pression des collaborateurs et assurer la continuité des activités pendant la pandémie de COVID-19, les entreprises ont considérablement développé le télétravail. Aujourd'hui, 91 % des collaborateurs qui utilisent un service IT travaillent au moins à temps partiel à domicile ou dans d'autres lieux distants.⁴ Seuls 9 % des collaborateurs sont retournés au bureau à temps plein. Ils sont également 9 % à travailler chez eux en permanence. La majorité des travailleurs (82 %) adoptent une approche hybride, combinant le travail au bureau et en dehors. En moyenne, 47 % des tâches salariales sont désormais réalisées hors du bureau physique.

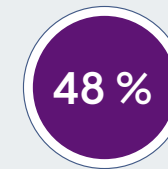
Depuis qu'ils ont découvert les avantages de l'« Everywhere Workplace » pendant la pandémie, la plupart des travailleurs sont réticents à retourner à plein temps au bureau. D'après une étude Ivanti,⁵ plus de 87 % des collaborateurs préfèrent une flexibilité leur permettant de travailler hors du bureau physique, tandis que 71 % affirment qu'ils préfèrent pouvoir travailler à distance plutôt qu'avoir une promotion. De plus, une grande partie des personnes interrogées disent avoir tiré des avantages personnels importants de la possibilité de travailler à distance, notamment :



mentionnent une amélioration de l'équilibre travail/vie privée



indiquent qu'ils peuvent ainsi réaliser des économies



disent avoir plus de temps pour travailler et pour la vie privée, en raison de l'absence de temps de trajet

Pour travailler efficacement, les collaborateurs doivent bénéficier de la même expérience numérique, qu'ils travaillent à distance ou qu'ils soient physiquement au bureau, notamment un accès facile aux systèmes et services IT. Pour cela, ils doivent pouvoir travailler de façon fluide sur des réseaux non professionnels (y compris des services Wi-Fi et Internet privés et publics) sans perte de connexion ou dépassement des délais de connexion. La qualité de la connexion réseau est déterminante pour les communications à distance comme la visioconférence.

Avec le télétravail, il est parfois difficile pour les administrateurs d'effectuer les tâches de dépannage, de remédiation et de maintenance des périphériques des collaborateurs. Ces derniers doivent pouvoir obtenir un niveau de service identique, quel que soit leur emplacement physique. Par ailleurs, il incombe aux entreprises de s'assurer que les périphériques utilisés et les services hébergés répondent aux exigences constantes de sécurité et de conformité.

⁴ « Identifying Effective Digital Employee Experience (DEX) Management Solutions: A Quantitative Analysis », 2021

⁵ « Everywhere Workplace Report », 2022

L'impact de la sécurité sur l'expérience collaborateur

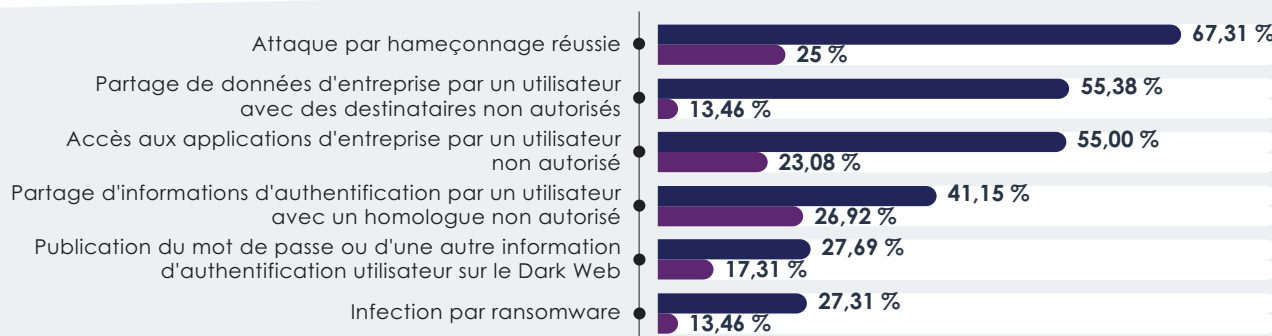
Paradoxalement, l'un des impacts sur l'expérience numérique des collaborateurs les plus négligés est aussi celui qui génère le plus de perturbations. Les exigences de sécurité de l'entreprise déconcentrent les utilisateurs et freinent les performances des postes client. Généralement, les entreprises considèrent la sécurité et l'expérience collaborateur comme des forces diamétralement opposées : quand vous augmentez l'une, vous diminuez l'autre. Adoptant ce point de vue, la plupart des entreprises favorisent la sécurité au détriment de la productivité des collaborateurs. Toutefois, une étude EMA montre qu'une réduction des mesures de sécurité contraignantes pour l'utilisateur entraîne une réduction significative des violations.⁶

Les inquiétudes liées à la sécurité sont tout à fait justifiées et les violations entravent considérablement les performances des collaborateurs. Par exemple, les infections

par malware et les attaques par ransomware endommagent les périphériques et bloquent l'accès à des ressources critiques. Les cookies de navigateur et les logiciels malveillants peuvent également permettre aux postes client d'effectuer des tâches non autorisées (comme le cryptojacking), ce qui réduit leurs performances. Une fois qu'un périphérique ou un compte de collaborateur est compromis, la remédiation du problème peut prendre beaucoup de temps, surtout si cela nécessite une restauration système complète, sans parler de l'impact sur la réputation et les finances de l'entreprise. Les événements de violation de sécurité peuvent aussi avoir un impact émotionnel sur les travailleurs car le stress induit a des effets sur leur productivité. Il est donc important de prendre conscience que la prévention des violations de sécurité, en tant que telle, est une méthode d'amélioration de l'expérience collaborateur.

Malheureusement, de nombreux processus courants de gestion de la sécurité ont également des répercussions négatives sur les tâches quotidiennes des collaborateurs. Les processus d'authentification contraignants (mots de passe, OTP 2FA, etc.) entravent l'accès aux principales ressources de l'entreprise. Les outils de tunneling réseau (comme les VPN) sont souvent lourds à utiliser mais indispensables pour obtenir un accès sécurisé aux systèmes d'entreprise. De plus, les processus de déploiement des correctifs de sécurité et les analyses antimalwares dégradent les performances des terminaux et entraînent souvent un redémarrage système.

Pour concilier sécurité et expérience collaborateur, les stratégies et les processus automatisés doivent être adaptables afin de s'ajuster aux besoins légitimes des utilisateurs finaux de l'entreprise.



- Répondants utilisant des processus de sécurité qui NUISENT à l'expérience collaborateur
- Répondants utilisant des processus de sécurité qui AMÉLIORENT l'expérience collaborateur

Comparaison du pourcentage des entreprises ayant connu un incident de sécurité au cours des 12 derniers mois selon le niveau de contrainte des processus de sécurité d'accès

⁶ « EMA Contextual Awareness Research Report », 2020

Les critères d'identification d'une solution performante

Pour mettre en place une solution DEX performante, il convient d'abord de s'assurer qu'elle répond aux nombreuses exigences en matière de support. La plupart des plateformes DEX du marché concentrent aujourd'hui leurs atouts sur un seul domaine ou certaines fonctions clés, comme la surveillance, l'analyse ou l'automatisation. Pour surmonter les lacunes de ces solutions, les entreprises s'appuient sur des intégrations avec des produits tiers ou développent des scripts d'automatisation personnalisés. Cependant, les plateformes DEX qui répondent le plus efficacement aux exigences uniques de l'entreprise sont celles qui prennent nativement en charge les fonctions clés des quatre piliers du support. Une approche unifiée de la DEX est plus facile à déployer et maintenir, avec à la clé un retour sur investissement rapide.

Les exigences des entreprises en matière de gestion de l'expérience numérique des collaborateurs évoluent sans cesse, et vous ne pouvez y répondre qu'avec une plateforme DEX unifiée fournissant les fonctions nécessaires pour surveiller les périphériques, déterminer le ressenti des collaborateurs, analyser les conditions d'utilisation et automatiser des réponses efficaces. Par exemple, la suite de solutions Ivanti Neurons offre une gamme complète et unifiée de fonctions DEX : visibilité en temps réel sur les périphériques, utilisateurs, applications et services IT, enquêtes flexibles

sur le ressenti des collaborateurs, etc. Ivanti Neurons offre une visibilité unifiée de l'expérience objective et subjective des collaborateurs. Des analyses et des calculs sont effectués à partir des informations collectées pour générer un score d'expérience utilisateur standardisé, et des « conseillers intelligents » (Smart Advisors) affichent des graphiques prédéfinis sur les conditions d'utilisation des périphériques et de l'environnement, avec des conseils pratiques sur les améliorations possibles et les actions correctives nécessaires.

Ivanti Neurons fournit des fonctions de remédiation entièrement automatisées. Des scripts d'autoréparation, appelés « bots », s'exécutent sur demande ou en continu en arrière-plan, et effectuent des opérations pour corriger les problèmes de performances, appliquer des changements de configuration et améliorer l'environnement. Bien que la plateforme comprenne une vaste bibliothèque de bots prédéfinis, elle inclut aussi un outil low code/no code facile à utiliser pour créer des workflows de bots personnalisés.

Les fonctions DEX d'Ivanti sont également entièrement extensibles, ce qui permet d'intégrer d'autres technologies Ivanti prenant en charge la gestion unifiée des terminaux (UEM), la gestion des correctifs, la gestion des services et la Spend Intelligence (intelligence des dépenses). Vous disposez aussi d'une bibliothèque de connecteurs pour une intégration directe avec des solutions de gestion tierces, comme ServiceNow, et il est possible de créer des intégrations personnalisées avec l'API REST fournie.

The screenshot displays the Ivanti Neurons interface for a device named 'sf-shha' (IP: 193.203.180.2). The interface is divided into several sections:

- General:** A table listing device attributes:

Device Name	Device Type	Device State
sf-shha	No Data	No Data
Assigned User	Login Name	Approximate Location
Shawn Holmstead	ENGR001sholmstead	No Data
Serial Number	Asset Tag	OS Name
02D4A87	No Data	Windows Server Enterprise
OS Version & Build	Windows Reliability	
No Data	No Data	
- Digital Experience Score:** Shows a 'Current Score' of 53 (Normal). It includes 'Potential Issues' such as 'Created On 4/14/2017 | 5 years, 2 months' and 'Warranty Out of warranty 12/14/2019'. A 'Last Calculated' timestamp of 3/11/2022, 2:05 PM is shown. Below the score, there are 8 Device Indicators: 2 Warning (red) and 6 Normal (green).
- Service Management:** Displays '0 Open Incidents' and '0 Incidents Last 30 Days'.
- Network:** Lists 'IP Address' (193.203.180.2), 'Connected to' (No Data), and 'Subnet Mask' (No Data). It also shows 'Default Gateway', 'MAC Address', and 'DHCP Enabled'.



À propos d'Enterprise Management Associates, Inc.

Fondé en 1996, Enterprise Management Associates (EMA) est un cabinet d'études leader du secteur, qui réalise des études de fond pour l'ensemble des technologies IT et de gestion des données. Les analystes EMA offrent une combinaison unique d'expérience pratique, d'informations sur les meilleures pratiques du secteur et une connaissance approfondie des solutions existantes et à venir des différents fournisseurs. Pour en savoir plus sur les services d'étude, d'analyse et de conseil d'EMA dédiés aux entreprises, aux professionnels de l'IT et aux fournisseurs IT, visitez le site www.enterprisemanagement.com. Vous pouvez aussi suivre EMA sur [Twitter](#) ou [LinkedIn](#).

Aucune copie, reproduction, opération de stockage dans un système de récupération ou retransmission de ce rapport, même partielle, n'est autorisée sans l'accord écrit d'Enterprise Management Associates, Inc. Toutes les opinions et estimations formulées dans ce rapport expriment notre jugement à la date de publication et sont susceptibles d'être modifiées sans préavis. Les noms de produits cités dans ce document sont des marques commerciales et/ou des marques déposées de leurs détenteurs respectifs. « EMA » et « Enterprise Management Associates » sont des marques d'Enterprise Management Associates, Inc. aux États-Unis et dans d'autres pays.

©2022 Enterprise Management Associates, Inc. Tous droits réservés. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES® et l'anneau de Möbius sont des marques déposées ou des marques de droit commun d'Enterprise Management Associates, Inc.