PRÉSENTATION

JANVIER 2025

Sécurisation des postes de travail : comment Dell aide à concilier l'adoption de l'IA et la cyber-résilience ?

Gabe Knuth, analyste senior

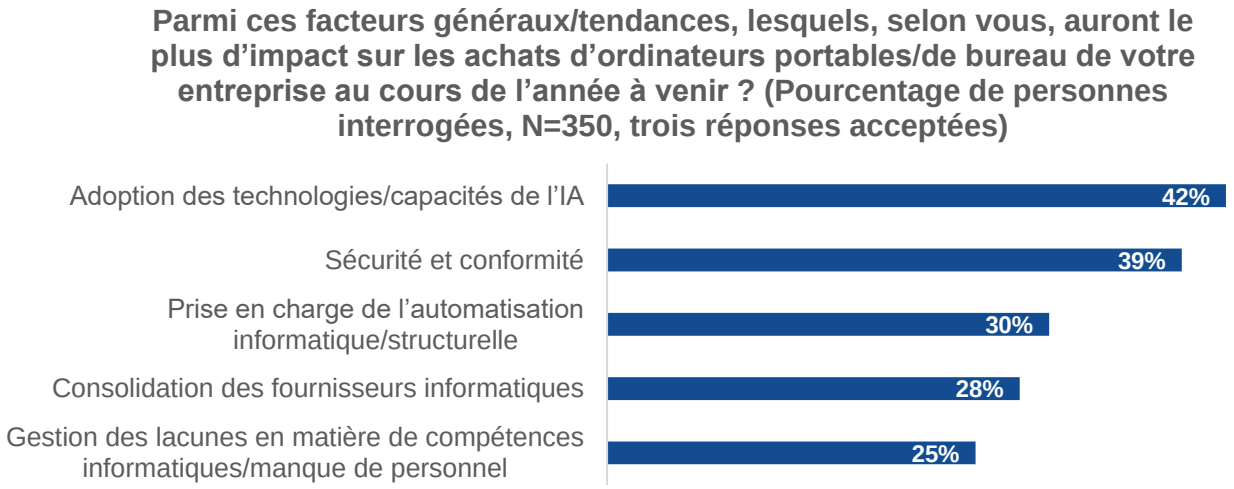
Résumé : Le rôle de la sécurité des postes de travail prend de plus en plus d'ampleur à mesure que l'adoption de l'IA à la fois par les entreprises et par les cybercriminels se développe. Une étude récemment menée par le groupe Enterprise Strategy Group d'Informa TechTarget met en évidence la double pression à laquelle les équipes informatiques sont confrontées : gérer des cybermenaces sophistiquées tout en permettant des innovations transformatrices.[1] Ce document explore comment la combinaison d'une sécurité sous le système d'exploitation, de pratiques sécurisées en matière de chaîne d'approvisionnement et de services complets font de Dell un partenaire de confiance pour les entreprises qui cherchent à renforcer leur stratégie de sécurité.

Présentation – Le problème

Alors que les entreprises sont confrontées à des cybermenaces en constante évolution, la sécurité est souvent la pierre angulaire de toute décision relative aux technologies. Cela vaut aussi bien dans le cloud et le datacenter que sur le PC, où, selon un récent projet de recherche d'Enterprise Strategy Group commissionné par Dell, la sécurité est l'une des principales caractéristiques influençant les achats d'ordinateurs de bureau et d'ordinateurs portables (voir Figure 1). Le plus frappant en l'occurrence est que les entreprises ont donné le même niveau de priorité à l'adoption des technologies et des fonctionnalités de l'IA, soulignant le fait qu'elles éprouvent des difficultés à intégrer des technologies transformatrices comme l'IA tout en protégeant leurs postes de travail contre les cybermenaces de plus en plus sophistiquées.

[1] Source : Enquête Enterprise Strategy Group Custom Research commissionnée par Dell, *Client Trends and Competitive Landscape*, juin 2024. Sauf indication contraire, toutes les références et tous les graphiques de la recherche menée par Enterprise Strategy Group exposés dans cette présentation proviennent de cette étude de recherche.

Figure 1 : Les 5 principaux facteurs affectant les achats de postes de travail



Source : Enterprise Strategy Group, une division d'Informa TechTarget

Cela n'a rien de surprenant. L'IA s'avérant déjà transformationnelle dans tout ce qui a trait aux utilisateurs, son ascension dans l'échelle des priorités était donc inévitable. Mais toutes les optimisations que l'IA apporte pour la productivité des utilisateurs, la créativité et les entreprises en général s'appliquent également aux utilisateurs malveillants, ce qui signifie que ce tandem entre l'adoption de l'IA et la sécurité (ou le trio, si vous comptez la conformité séparément) est probablement loin de disparaître.

Alors que de nombreuses entreprises sont encore en train de définir l'utilisation de l'IA et les préoccupations qu'elle génère, les défis liés à la sécurité sont bien compris, notamment les suivants :

- Suivi des cycles de mise à niveau matérielle et logicielle (cité par 32 % des personnes interrogées)
- Sécurisation des données confidentielles sur les ordinateurs portables et de bureau (29 %)
- Création d'un environnement de travail hybride (27 %)
- Prise en charge du nombre croissant d'utilisateurs finaux (27 %)
- Gestion des correctifs (20 %)
- Gestion de l'utilisation non autorisée des applications ou des modifications de configuration (17 %)

Ces défis « classiques », associés à l'émergence de l'IA et aux attaques toujours plus nombreuses et sophistiquées, dressent un tableau peu enviable de l'informatique. En vérité, il est impossible de tout bloquer, d'où l'importance de tirer parti de tous les outils disponibles pour garder une longueur d'avance sur les défis d'aujourd'hui et sur ceux qui se profilent.

Que peuvent faire les entreprises ?

Pour relever ces défis, les entreprises doivent tirer parti des fonctionnalités de sécurité qui peuvent les aider à développer leurs initiatives en cours. Souvent, cela signifie aller au-delà des mesures de sécurité de base et de la formation des utilisateurs finaux, en choisissant plutôt de se concentrer sur une approche multicouche élargie qui peut aider à renforcer la cyber-résilience à long terme.

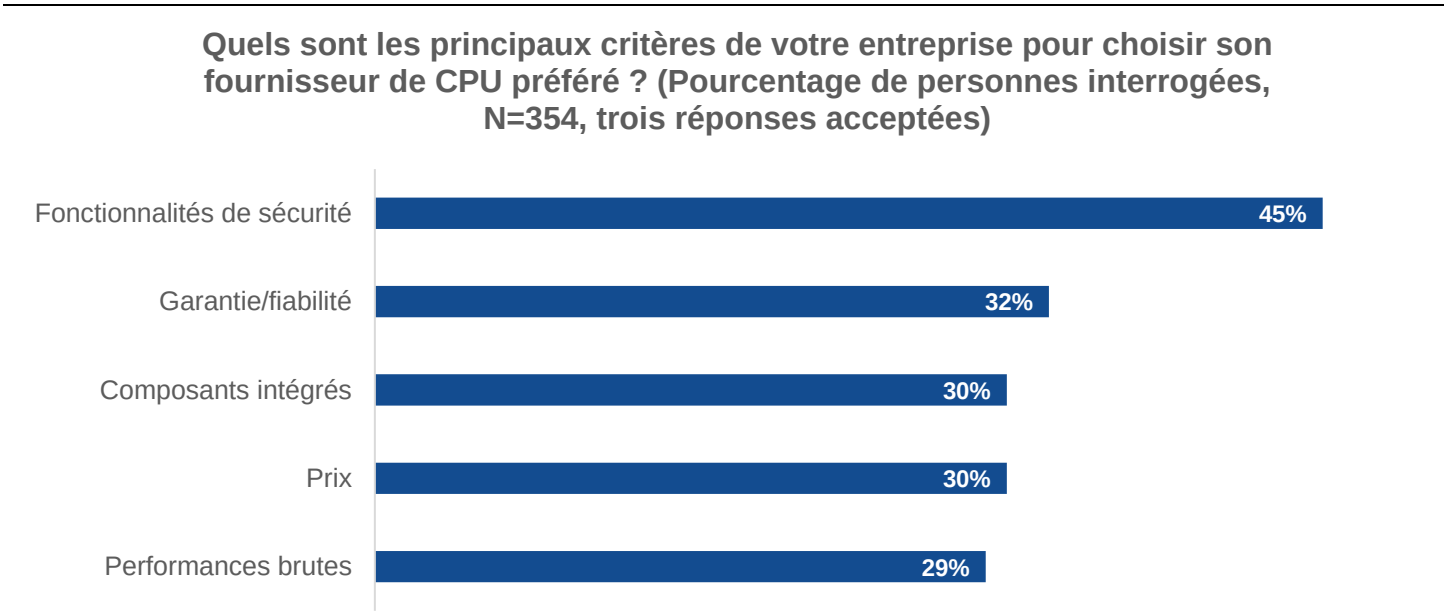
L'un des aspects est souvent négligée (ou du moins minimisée) : le rôle joué par la sécurité matérielle ou « sous le système d'exploitation ». La sécurité matérielle réduit la surface d'attaque globale d'une machine, ce qui peut atténuer les attaques avant qu'elles n'aient la possibilité de s'établir. Une sécurité de base renforcée

vient compléter les outils logiciels de configuration, d'analyse et de correction, ce qui réduit la charge pesant sur les ressources informatiques qui analysent en permanence les alertes et problèmes détectés.

Si le matériel est si puissant, alors pourquoi est-il si souvent négligé ? Trop souvent, le matériel est considéré comme un produit classique, un mal nécessaire qui nécessite l'application de correctifs et des opérations de maintenance ou, pire encore, qui est déployé et que l'on oublie. En réalité, chaque génération de chipsets est dotée de fonctionnalités de sécurité plus avancées qui peuvent protéger contre les attaques au niveau du micrologiciel et du matériel. Depuis peu, le matériel dispose de mesures de sécurité intégrées qui peuvent fonctionner avec les outils de sécurité intégrés au système d'exploitation pour détecter tout comportement anormal au sein des applications.

Alors que la mise à jour d'un appareil ou de son micrologiciel était historiquement perçue comme nécessaire uniquement en cas d'obsolescence ou de problème, la réalité est que ces mises à jour améliorent souvent la stratégie de sécurité globale, d'autant plus qu'elles sont destinées aux appareils des utilisateurs finaux ! C'est pour cette raison que les fonctionnalités de sécurité figurent en tête de liste des critères décisifs pour choisir un fournisseur de CPU (voir Figure 2).[2]

Figure 2. Les 5 principaux facteurs influençant le choix de fournisseur de CPU



Source : Enterprise Strategy Group, une division d'Informa TechTarget

Il existe également des éléments de sécurité qui ne sont pas souvent pris en compte par les administrateurs, notamment la sécurité de la chaîne d'approvisionnement, qui a été citée par 40 % des entreprises comme l'un de leurs principaux défis lors de l'achat d'ordinateurs portables/de bureau (derrière la gestion des coûts, les demandes croissantes des utilisateurs finaux et la vitesse d'exécution).

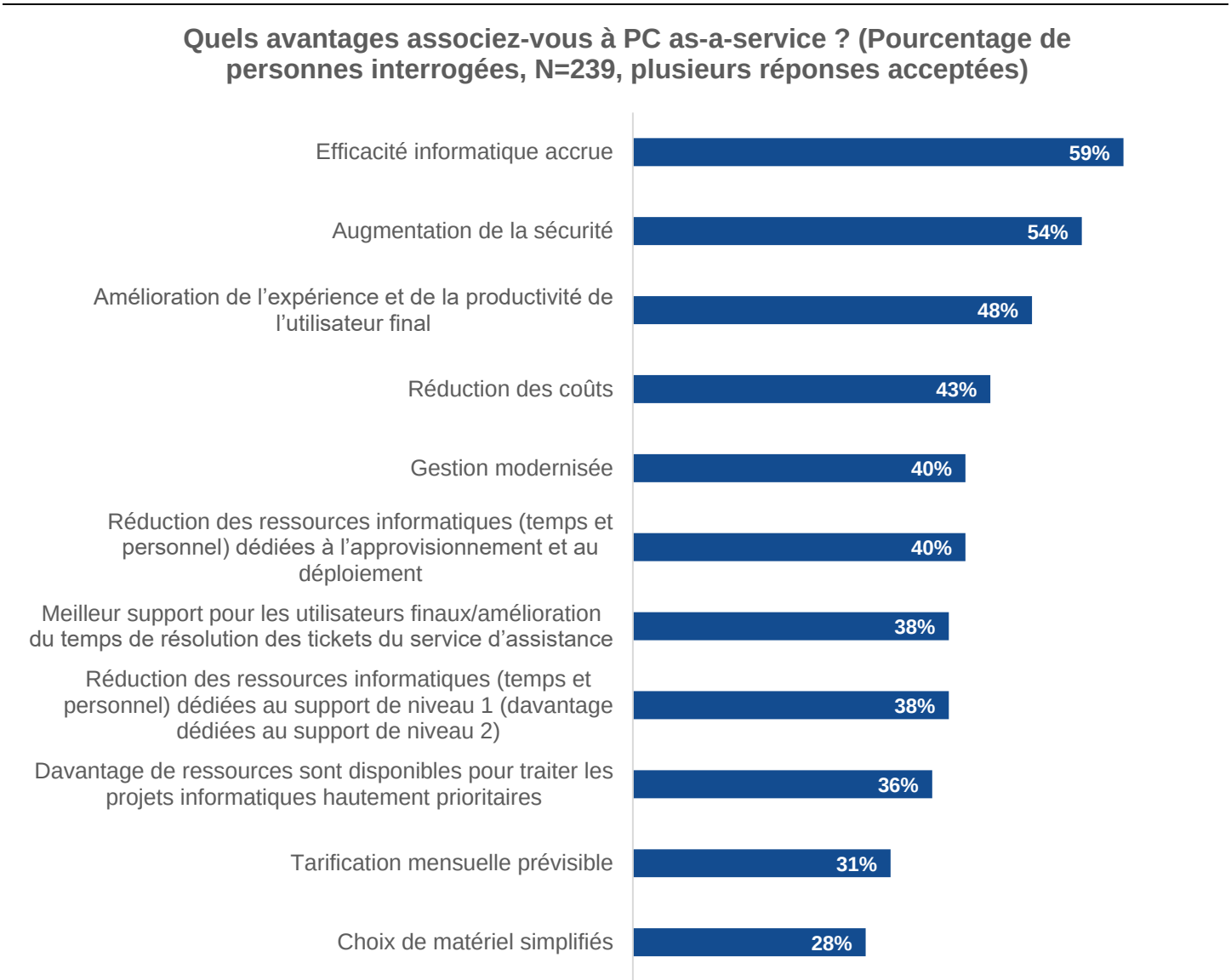
Dans l'ensemble, cela met en évidence la nécessité pour les entreprises de travailler avec des fournisseurs qui font preuve de dévouement envers la sécurité matérielle et celle de la chaîne d'approvisionnement. Cela facilitera certainement l'achat, mais si l'on se souvient des 32 % des entreprises qui ont du mal à suivre les cycles de mise à niveau normaux ou des 20 % qui ont indiqué avoir des difficultés à gérer les correctifs, cela

[2] Source : Résultats complets de l'enquête Enterprise Strategy Group, *Endpoint Device Trends*, février 2024.

suggère que les entreprises pourraient également avoir besoin d'aide pour les tâches de sécurité quotidiennes.

En conséquence, il n'est pas surprenant de voir les entreprises miser de plus en plus sur des services gérés comme PC as-a-Service (PCaaS). PCaaS simplifie l'achat et le support en offrant différents appareils et niveaux de service moyennant un coût d'exploitation mensuel. Dans le cadre de l'enquête, les personnes interrogées qui utilisent PCaaS ont été questionnées sur les principaux avantages qu'elles associent à ce service. Parmi les réponses occupant une place prépondérante dans les résultats, on retrouvait une meilleure efficacité informatique (59 %), une sécurité accrue (54 %) et une meilleure expérience/productivité des utilisateurs finaux (48 %) (voir Figure 3), montrant ainsi que les services peuvent également jouer un rôle clé dans une approche de sécurité multicouche.

Figure 3. PCaaS présente de nombreux avantages, notamment une sécurité accrue



Source : Enterprise Strategy Group, une division d'Informa TechTarget

Comment Dell peut vous aider ?

En tant que leader dans tous les domaines abordés jusqu'à présent (IA, sécurité, expérience utilisateur, etc.), Dell occupe une position unique pour aider ses clients à atteindre leurs objectifs. Dell comprend que la sécurité doit être assurée tout au long du cycle de vie des appareils, de la chaîne d'approvisionnement au recyclage. Dell assure un contrôle strict de sa chaîne d'approvisionnement, garantissant sécurité et disponibilité grâce à divers fabricants de puces, sites et canaux de distribution à l'échelle mondiale.

Ses PC et ordinateurs portables commerciaux offrent une sécurité sous le système d'exploitation via Dell Trusted Device et Dell SafeBIOS, une suite de fonctionnalités qui protège l'intégrité des appareils jusqu'au niveau du BIOS et du micrologiciel. Cette fonctionnalité, associée à la puce de silicium Intel Core, signifie que les appareils commerciaux Dell offrent une sécurité matérielle complète qui minimise la zone d'attaque de chaque appareil. Cette combinaison d'appareils Dell Trusted Device alimentés par des processeurs Intel est l'une des raisons pour lesquelles Dell est reconnu comme un leader en matière de sécurité des postes de travail. Dell inclut également ses propres logiciels pour s'assurer que le micrologiciel, le BIOS et les pilotes des appareils restent à jour, ce qui est particulièrement décisif pour les entreprises qui ont du mal à gérer les correctifs et l'utilisation non autorisée des applications.

Enfin, Dell offre une gamme flexible de services pour soutenir les entreprises dépassées par les exigences croissantes en matière de gestion de la sécurité des postes de travail. ProSupport et ProSupport Plus fournissent une assistance technique avancée et une résolution prédictive des problèmes, garantissant ainsi la sécurité et le fonctionnement des appareils avec un temps d'arrêt minimal. Pour les entreprises qui cherchent à simplifier davantage leurs opérations informatiques, Dell APEX PC-as-a-Service (APCaaS) offre une solution complète en regroupant le matériel, les logiciels et les services de cycle de vie dans un modèle par abonnement prévisible.

Cette approche holistique, associant une chaîne d'approvisionnement sophistiquée, un matériel de pointe, des logiciels robustes et des services flexibles, donne aux entreprises la longueur d'avance dont elles ont besoin pour surmonter les problèmes de sécurité associés aux postes de travail actuels, en permettant aux équipes informatiques de maintenir une stratégie de sécurité solide, malgré une complexité croissante et des ressources limitées.

Conclusion

Pour les équipes informatiques, la sécurité est un défi constant qui ne cesse de prendre de l'ampleur, une même technologie pouvant autant stimuler les entreprises qu'aider les utilisateurs malveillants. Mais ce n'est pas forcément une bataille perdue d'avance. Malgré l'ascension des tendances émergentes comme l'IA dans la liste des priorités, il est important de se focaliser sans relâche sur la nécessité d'assurer une sécurité complète des postes de travail. Les entreprises peuvent prendre des mesures clés pour relever leurs défis en élaborant une approche multicouche qui tire parti du matériel, des logiciels et des services.

Souvent, cela implique de travailler avec des partenaires de confiance, ce qui explique pourquoi le portefeuille de Dell se démarque. Dell se concentre sur la sécurité matérielle, la protection du cycle de vie de bout en bout et des offres de services flexibles. Ainsi, les clients disposent des outils et du support dont ils ont besoin pour traiter les tâches de sécurité quotidiennes et atteindre leurs objectifs stratégiques à long terme d'améliorer la sécurité tout en adoptant et profitant des technologies émergentes. En somme, les solutions Dell sont adaptées aux exigences des environnements informatiques modernes.

Dans un monde où l'IA et la sécurité sont devenues tout aussi prioritaires l'une que l'autre, les entreprises doivent adopter des stratégies qui font des postes de travail un outil de productivité et un élément clé des objectifs de cybersécurité des entreprises. La capacité de Dell à combiner ces priorités dans une approche unifiée en fait un choix naturel pour les entreprises qui valorisent l'innovation, la fiabilité et la tranquillité d'esprit.

Pour plus d'informations, rendez-vous sur le site dell.com/endpoint-security.

À propos d'Enterprise Strategy Group
Enterprise Strategy Group de TechTarget fournit des informations sur le marché ciblées et exploitables, des recherches axées sur la demande, des services de conseil aux analystes, des conseils sur la stratégie de mise sur le marché, des validations de solution et du contenu personnalisé pour accompagner l'achat et la vente de technologies d'entreprise.

contact@esg-global.com
www.esg-global.com