Construisez des bases solides pour votre IT et votre sécurité

Les 3 leviers d’une compréhension complète de votre parc IT

À l'ère du travail hybride, le département IT joue un rôle essentiel dans l'entreprise. La plupart des collaborateurs sont dépendants de l'IT pour réaliser leurs tâches quotidiennes. Devant la généralisation du travail en ligne, le parc IT s'est complexifié.

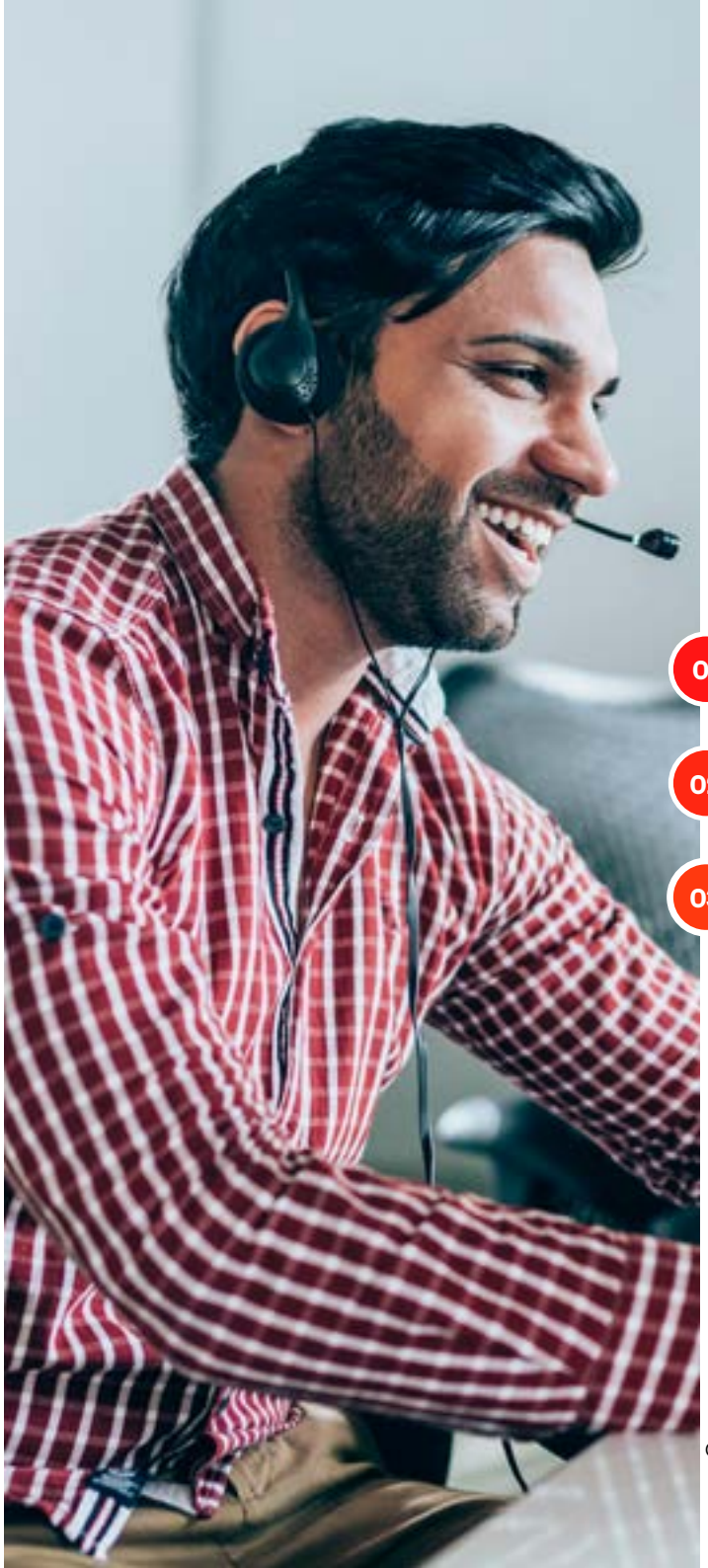
Aujourd'hui, les collaborateurs utilisent en moyenne 2,6 périphériques[1] pour travailler.

Cela représente une multitude de postes client qu'il faut cartographier, surveiller, sécuriser et maintenir proactivement. De plus, IDC prévoit que[2], d'ici 2025, les périphériques connectés en périphérie généreront **79,4 zettaoctets** de données.

En matière d'IT et de sécurité, il est indispensable d'avoir une bonne **compréhension de votre parc IT**. Cette connaissance est un atout inestimable qui va au-delà de ce que peut vous apporter une base CMBD propre.

1 «L'évolution des exigences de la DEX (Gestion de l'expérience numérique), EMA, 2022

2 « Worldwide Global DataSphere IoT Device and Data Forecast, 2019-2023 », 2019-2023, IDC



01 **Améliorer le support et la gestion des services**

02 **Améliorer la visibilité et la sécurité des informations**

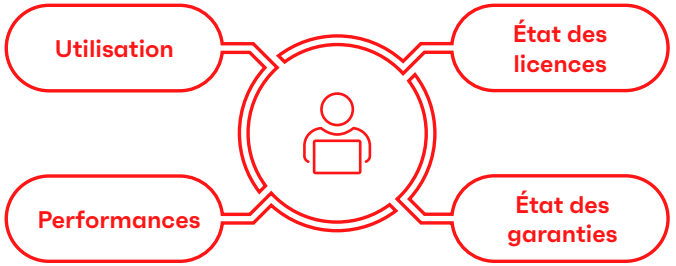
03 **Mieux contrôler la gestion des coûts**

01

Améliorer le support et la gestion des services

Dans un environnement IT de plus en complexe, l'équipe de support doit prendre en charge un nombre croissant de périphériques (certains accédant au réseau de façon non contrôlée). Résultat : une augmentation des problèmes potentiels et réels, qui se traduit par une avalanche de tickets de support.

C'est dans ce contexte qu'une bonne compréhension de votre parc IT bénéficie à vos équipes de gestion des services et de support en première ligne. En centralisant les données relatives aux actifs (utilisation, performances, licences et état de la garantie), vous faites un pas vers une **approche proactive** qui permet de résoudre les problèmes avant qu'ils n'impactent l'utilisateur final.



Que se passe-t-il lorsqu'un ticket est créé ? Les informations sur les actifs étant centralisées, votre centre de support dispose de tout le contexte nécessaire pour résoudre l'incident bien plus rapidement, **sans qu'il soit nécessaire de l'escalader.**

Avec des données contextualisées exhaustives sur l'ensemble de votre parc IT, vos équipes Support IT et Gestion des services sont en mesure de **prendre plus rapidement des décisions plus pertinentes qui améliorent l'expérience collaborateur et la productivité.**

02

Améliorer la visibilité et la sécurité des informations

On ne peut corriger que ce qu'on connaît. Avec la multiplication des périphériques connectés, des tâches manuelles telles que la surveillance et l'audit des périphériques sont pratiquement impossibles, du moins pas en temps réel.

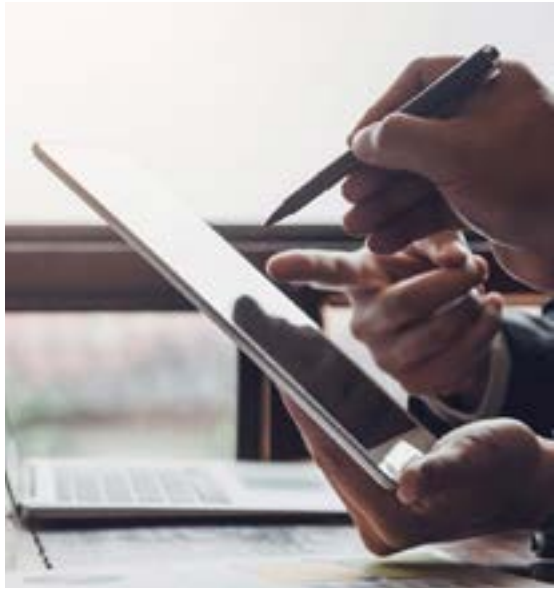
Le coût moyen d'une fuite de données peut atteindre

4,35 millions de dollars[1]

Avec l'augmentation du coût moyen d'une fuite de données (jusqu'à 4,35 millions de dollars) et l'allongement d'année en année des périodes d'inactivité, votre équipe Sécurité IT doit savoir à tout moment quels sont les périphériques qui accèdent au réseau de votre entreprise. Maintenir la **conformité et la sécurité des données** sans impacter l'expérience numérique collaborateur est beaucoup plus facile lorsque les informations sur vos actifs sont centralisées dans une vue unique.

Aux États-Unis, le CIS (Center for Internet Security)[2] définit 18 contrôles de sécurité critiques, dont les deux plus importants sont l'inventaire et le contrôle des actifs d'entreprise, et l'inventaire et le contrôle des actifs logiciels. En appliquant les **cinq premiers** contrôles, vous prévenez **85 % des cyberattaques**.

Dans l'UE, l'ENISA[3] offre une couverture similaire, répartie sur 27 points de contrôle. Ce n'est que lorsque ces critères sont satisfaits que les administrateurs sont correctement équipés pour appliquer d'autres contrôles de sécurité



critiques, comme la protection des données et la gestion du contrôle d'accès.

Ces deux contrôles de sécurité fondamentaux englobent l'inventaire, le suivi et la correction de tous les actifs de l'entreprise, y compris les actifs physiques comme les périphériques mobiles, et les actifs logiciels comme les systèmes d'exploitation et les applications. Une bonne compréhension de l'intégralité de votre environnement IT vous permet de vous assurer que seuls les logiciels autorisés sont installés et exécutés, et que tous les nouveaux actifs connectés à votre réseau sont **automatiquement identifiés et analysés.**

1 Cost of a Data Breach 2022 Report, IBM

2 The 18 CIS Critical Security Controls, Center for Internet Security

3 Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA

03

Mieux contrôler la gestion des coûts

La gestion des dépenses IT n'a jamais été aussi difficile. Sachant que l'évolutivité et l'agilité sont des leviers stratégiques et que le département IT est l'épine dorsale de l'entreprise, il est indéniable que la gouvernance des architectures multiclouds pose un réel défi.

32 % **des professionnels de l'IT pensent que 10-25 % des dépenses IT sont gaspillées pour des logiciels non utilisés, sous-utilisés, non gérés ou non pris en compte.[1]**

Avec une meilleure compréhension des données d'utilisation des actifs dans l'environnement IT, l'entreprise gère mieux son budget IT et vos équipes **optimisent l'utilisation des actifs**. Par exemple, si vous disposez d'informations détaillées telles les licences logicielles, les garanties, les contrats, les actifs physiques et virtuels, et les services Cloud, vous êtes à même de **décider rapidement si une machine doit être réparée ou retirée.**

En contrôlant mieux les coûts, vous **optimisez aussi la gestion des licences**. Compte tenu de l'énorme dépendance envers les actifs IT sur abonnement, vous gagnerez à disposer d'informations sur les licences inutilisées ou manquantes et sur les abonnements Cloud pouvant être annulés. Cela se traduira par des réductions de coûts et des risques d'amende réduits.

Comme toutes ces informations sont réunies au même endroit, votre centre de support peut prendre des décisions en toute connaissance de cause, par exemple pour répondre à une demande d'accès à une application. Au lieu d'acheter encore un accès de plus, l'équipe peut réallouer celui que vous payez déjà alors que personne ne l'utilise.

1 Modern ITAM in the Digitally-Transformed Enterprise, Enterprise Management Associates, 2022

Bien plus que la visibilité

La compréhension de l'ensemble de votre parc IT va **bien au-delà de la simple découverte et de la visibilité** des actifs sur votre réseau. Le véritable avantage réside dans le fait de considérer cela comme une base pour améliorer votre support IT et la gestion de vos services, renforcer votre sécurité, améliorer l'expérience des collaborateurs et optimiser vos dépenses IT. Pour un Everywhere Workplace fluide et réussi, il est essentiel de disposer d'un lieu unique qui centralise toutes les informations sur votre environnement IT .

Construisez des bases solides pour votre IT et votre sécurité

Les 3 leviers d'une compréhension complète de votre parc IT

ivanti.fr
+33 (0)1 76 40 26 20
contact@ivanti.fr