



ivanti

# Une meilleure visibilité, des données précises, des décisions plus pertinentes

De meilleures infos IT pour de meilleurs résultats d'entreprise

## Table des Matières

Introduction	3
Manque de visibilité : Six études de cas	4
1: Des ordinateurs portables au ralenti	4
2: Routeurs sur le quai de reception	5
3: Économies de bouts de chandelle	7
4: « Snail Mail » ou « Courrier escargot »	8
5: Verrouillage d'un ordinateur portable	10
6: Un univers IT inconnu	11
Ivanti : Pour avoir des yeux derrière la tête	12

Ce document est fourni uniquement à titre d'information. Aucune garantie ne pourra être fournie ni attendue. Ce document contient des informations confidentielles et/ou qui sont la propriété d'Ivanti, Inc. et de ses sociétés affiliées (désignés collectivement ici sous le nom « Ivanti »). Il est interdit de les divulguer ou de les copier sans l'autorisation écrite préalable d'Ivanti.

Ivanti se réserve le droit de modifier le présent document, ou les caractéristiques produit et descriptions associées, à tout moment et sans avis préalable. Ivanti n'offre aucune garantie pour l'utilisation du présent document, et refuse toute responsabilité pour les éventuelles erreurs qu'il contient. Ivanti n'est pas non plus tenu de mettre à jour les informations de ce document. Pour consulter les informations produit les plus récentes, visitez le site [ivanti.fr](http://ivanti.fr)

## Introduction

Même si vous oubliez tout le reste de ce livre blanc, gardez ceci à l'esprit :

Disposer d'une visibilité complète de vos biens et services IT, de votre position en matière de sécurité, de vos processus et de vos résultats constitue la base pour correctement gérer, sécuriser et optimiser votre parc IT. Si vous y voyez plus clair, vous prenez de meilleures décisions et devenez plus efficace. Cela vous aide à optimiser les coûts et les futurs budgets, à améliorer l'expérience de vos clients et collaborateurs, et à positionner votre équipe pour plus de productivité et d'efficacité.

C'est ce que tout le monde veut, dans notre environnement actuel d'industries très réglementées et d'obligations de conformité. Il est nécessaire de définir une direction claire pour l'application des correctifs, l'optimisation des coûts, le contrôle des applications et la localisation des biens. De plus, l'objectif du département IT est de « s'asseoir à la table ronde » et de devenir un centre d'innovation, au lieu d'un simple centre de coûts.

Pour être honnête, il faut plusieurs étapes pour atteindre une visibilité complète :

- Si vous ne définissez pas votre point de départ

de référence, comment savoir quelles sont vos perspectives concernant les biens, la sécurité, les processus et la maturité, ou la quantité de travail et le type de tâche qui attendent le département IT ?

- Comment gérer ce que vous ne connaissez pas dans votre environnement IT ?
- Comment générer une plus grande valeur ajoutée pour l'entreprise avec un budget et des ressources IT inchangés ?
- Comment assurer un support étendu pour un éventail de périphériques toujours plus large ?

## Ivanti met en lumière tous les recoins du parc IT de votre entreprise

L'amélioration de la visibilité doit devenir une pratique de fonctionnement de base, et les solutions éprouvées d'Ivanti braquent un projecteur sur tous les aspects du parc IT de votre entreprise. L'approche « IT unifiée » rassemble les équipes IT des départements Gestion des services IT (ITSM), Gestion des biens IT (ITAM), Gestion de la sécurité du poste client et Gestion des utilisateurs et des espaces de travail (UWM), sous l'égide des solutions Enterprise Service Management (ESM - Gestion des services d'entreprise) et Unified Endpoint Management (UEM - Gestion unifiée des postes client). Comme ces solutions apportent

davantage de clarté et de visibilité, vous êtes davantage synchronisé avec vos utilisateurs, vos services et vos biens dans toute l'entreprise, ainsi qu'avec votre environnement IT, votre position en matière de sécurité, vos processus et vos données. Cela vous donne les moyens d'atteindre un plus grand nombre d'objectifs stratégiques.

## À propos de ce livre blanc

Ce livre blanc fournit six brefs scénarios et des résultats de recherche, pour vous aider à déterminer les points sur lesquels votre département IT pourrait gagner en clarté et en visibilité. De plus, il vous invite à évaluer les solutions Ivanti qui ont fait leurs preuves en aidant des entreprises à y parvenir.





# Manque de visibilité : Six études de cas

Examinez les six scénarios ci-après, qui montrent les difficultés généralement associées à un manque de visibilité :

1

## Des ordinateurs portables au ralenti

Un agent du centre de support remarque un accroissement des appels concernant des incidents liés au ralentissement des ordinateurs portables. Après de nombreux appels de suivi qui lui prennent beaucoup de temps, l'agent apprend qu'un cadre est revenu d'une conférence une semaine plus tôt, avec ce qu'il appelait une « appli qui tue », et qu'il a encouragé les autres personnes à télécharger cette application depuis sa clé USB, en réutilisant la même licence. D'autres investigations montrent aussi que l'application est une grosse consommatrice de ressources, mais on ne sait pas vraiment sur combien d'ordinateurs portables elle a été installée.

Aujourd'hui, de nombreux départements IT appliquent des procédures immatures et/ou manuelles, qui limitent la visibilité dans l'ensemble de l'entreprise. Sans une bonne visibilité, il est très difficile de détecter, de gérer et de sécuriser le matériel et les logiciels, et de gérer efficacement l'utilisation des logiciels.

Le scénario ci-dessus comprend plusieurs inconnues :

- Risque de non-conformité en raison de l'utilisation d'un logiciel sans licence.
- Shadow IT : les collaborateurs contournent le département IT et installent des logiciels non autorisés.
- Nombre d'ordinateurs portables susceptibles d'être concernés.
- Nombre total d'incidents liés à venir.
- Risques de sécurité créés par l'installation et l'utilisation de logiciels non autorisés.
- Incertitude concernant les risques de frais de mise en conformité des licences.

Pour insister sur le fait qu'il est impossible de gérer, de protéger et d'optimiser les éléments que vous n'êtes pas conscient de posséder ou que vous ne pouvez pas

# 43 %

des entreprises interrogées utilisent encore des feuilles de calcul.

# 50 %

utilisent une solution de gestion du poste client.

# 45 %

utilisent différentes ressources, dont des outils d'inventaire.

voir, le livre blanc Ernst & Young (EY) intitulé « Data Validation the Best Practice for Data Quality in Fixed Asset Management » montre que 56 % des entreprises vérifient l'emplacement de leurs biens fixes seulement une fois par an, tandis que 10 à 15 % n'ont pas vérifié leurs biens depuis plus de cinq ans.

Sans programme formel de gestion des biens IT (ITAM), les équipes comptent souvent uniquement sur Active Directory ou des données d'inventaire de base provenant d'une solution de gestion du poste client. Concernant le suivi des biens, l'enquête ITXM mandatée par Ivanti en décembre 2019 donne les résultats suivants. Notez que certaines entreprises sont concernées par plusieurs de ces affirmations :

Combiner plusieurs sources de données (telles que les données ITSM, ITAM et SAM par exemple), demande plus de temps pour réunir les informations nécessaires et disposer d'une visibilité globale. Selon une enquête Enterprise Management Associates (EMA), 50 % des entreprises emploient au moins 12 outils de découverte et/ou d'inventaire, et 11 % en utilisent plus de 30. En moyenne, les entreprises passent 10 heures par semaine à résoudre les problèmes d'inexactitude des données. 32 % y consacrent même plus de 25 heures par semaine.

En bref, le manque de visibilité signifie que vous ne pouvez pas gérer, protéger et optimiser les éléments que vous ne connaissez pas ou que vous ne visualisez pas facilement. Les solutions Ivanti comportent de puissantes fonctions d'importation de données,

qui vous permettent de combiner les données de plusieurs sources (feuilles de calcul, outils d'inventaire, lecteurs de code-barres, services de découverte, etc.) pour comparer les données réelles aux données découvertes et signaler les écarts. Grâce à ces informations, les décideurs peuvent confirmer leurs hypothèses et s'assurer que les informations liées aux biens IT sont toujours à jour et exactes.

## 2

### Routeurs sur le quai de réception

L'équipe Opérations réseau reçoit un appel du quai de réception. Une palette de nouveaux routeurs vient d'arriver. L'équipe Opérations commence à configurer les nouveaux routeurs pour remplacer certains des anciens, avant de se rendre compte que personne n'avait, en fait, commandé ces nouveaux routeurs.

Le manque de visibilité génère de nombreuses inconnues. Quel est l'historique d'approvisionnement ? Quels sont les fournisseurs et méthodes d'approvisionnement favoris ? Quels sont les risques de sécurité potentiels liés à la connexion de matériel non autorisé au réseau ?

# 39 %

des entreprises interrogées utilisent plusieurs systèmes et référentiels.

# 38 %

effectuent manuellement le suivi de ces informations, dans leurs feuilles de calcul d'inventaire.

# 37 %

effectuent ce suivi dans leur référentiel/base de données de gestion des biens.

# 22 %

utilisent un système de gestion des contrats séparé.

L'enquête ITXM, mentionnée ci-dessus, mandatée par Ivanti en décembre 2019, cherchait à connaître les méthodes utilisées par les entreprises pour suivre et surveiller les données d'achat, les contrats et les données de garantie de leurs biens IT. Les résultats de l'enquête sont les suivants. Là encore, notez que certaines entreprises sont concernées par plusieurs de ces affirmations :

Une bonne visibilité des données et de leurs sources (savoir quelles sont les données et les avoir toutes au même endroit) permet de résoudre un grand nombre des difficultés évoquées ci-dessus. Cela permet d'obtenir des données cohérentes, précises et exactes.

Comme mentionné dans notre introduction, lorsque la Gestion des Services d'Entreprise (ESM – Enterprise Service Management) et la Gestion Unifiée du Poste Client (UEM - Unified Endpoint Management) sont étroitement alignés, intégrés et automatisés, vous pouvez :

- Utiliser les informations de découverte des biens pour émettre des prévisions et prendre des mesures par anticipation concernant les types de biens qui posent problème, les modèles et les fournisseurs.
- Obtenir des informations plus détaillées, permettant d'améliorer la gestion des fournisseurs, la conformité et l'optimisation des garanties.
- Libérer vos ressources IT des activités réactives ou opération inutiles et leur donner la possibilité de se concentrer sur des projets plus stratégiques.
- Réduire les risques de sécurité en sachant quel matériel est autorisé à être utilisé.
- Accomplir plus tout en minimisant les coûts et les efforts administratifs, ce qui apporte davantage de valeur ajoutée à l'entreprise.

### 3

## Économies de bouts de chandelle

Le directeur IT demande à son personnel de trouver des façons de faire des économies de budget pour l'année en cours. Le vice-président Opérations veut savoir s'il est possible de retarder le cycle de renouvellement des ordinateurs portables, mais personne ne sait combien d'ordinateurs portables sont concernés, les collaborateurs que cela va impacter, les problèmes potentiels que cela va créer et le montant des économies réelles réalisées.

Dans ce scénario, les difficultés qui surgissent sont notamment le manque de visibilité sur les ordinateurs portables et à l'historique fournisseur, l'absence de suivi cohérent de l'ensemble du cycle de vie du bien pour connaître l'état de santé et les performances des

ordinateurs portables, et l'absence d'historique connu concernant l'application des correctifs. On ne sait pas non plus quels collaborateurs seront impactés.

Avec des informations appropriées, l'un des clients Ivanti a pu étendre le cycle de renouvellement de son matériel de six à douze mois, faisant ainsi économiser au département IT un montant initial de 1,5 million de dollars, sans aucune augmentation du taux d'incidents ni aucun impact sur la qualité de service pour les utilisateurs finaux.

En outre, l'enquête ITXM de décembre 2019 a montré que :

La compréhension du cycle de vie, des performances, de la conformité et des implications de coût des biens est particulièrement importante pour les entreprises des secteurs les plus réglementés. C'est le cas par exemple du secteur des périphériques médicaux, avec la norme MDR (Règlement relatif aux dispositifs médicaux) et la base de données associée EUDAMED (Base de données européenne du dispositif médical) dans l'Union européenne.

# 28 %

des professionnels de l'IT interrogés passent des heures, chaque semaine, à assurer le support de biens hors garantie ou dont le contrat de support n'est plus actif.

# 20 %

d'entre eux disent qu'ils n'ont pas d'informations sur les biens obsolètes.

# 4

## « Snail Mail » ou « Courrier escargot »

Dès son arrivée un matin, le personnel du centre de support est submergé par une vague d'appels de collaborateurs. Les e-mails « ne fonctionnent pas » ou « sont vraiment très lents ». Après plusieurs appels aux autres équipes IT, l'équipe Opérations IT conclut qu'une personne a mis à jour l'application d'e-mail pendant la nuit et que le serveur actuel n'est pas capable de gérer les changements de configuration qui en résultent, créant ainsi des problèmes de performances. On ne sait pas immédiatement si l'équipe dispose du matériel nécessaire pour résoudre ce problème.

Dans ce cas, les difficultés provoquées par le manque de visibilité sont le manque de clarté de l'historique des changements et des configurations, le manque de connaissance des changements futurs, l'absence d'analyse de l'impact et des risques de ces changements, et l'absence d'historique d'inventaire.

Les entreprises mettent en place des objectifs IT pour améliorer leur niveau de maturité et font appel à l'automatisation pour gagner en efficacité. Et pourtant, un grand nombre oublie l'étape de départ indispensable : définir le point de départ de référence. Cela signifie : 1) Obtention d'une visibilité complète des processus et actions qui affectent les principaux services et les biens sous-jacents, comme la gestion des changements ; et 2) compréhension totale des schémas d'incident, de la cause des coupures, etc. afin de définir la situation de référence à améliorer.

Le fait est que, en dépit des efforts des équipes IT, des systèmes peu performants et le manque

de ressources peuvent nuire à la qualité tactique et réactive des activités de service et de support. Aucune approche systématique n'est imposée pour aller au-delà des résultats à court terme et les problèmes sont résolus au coup par coup. En outre :

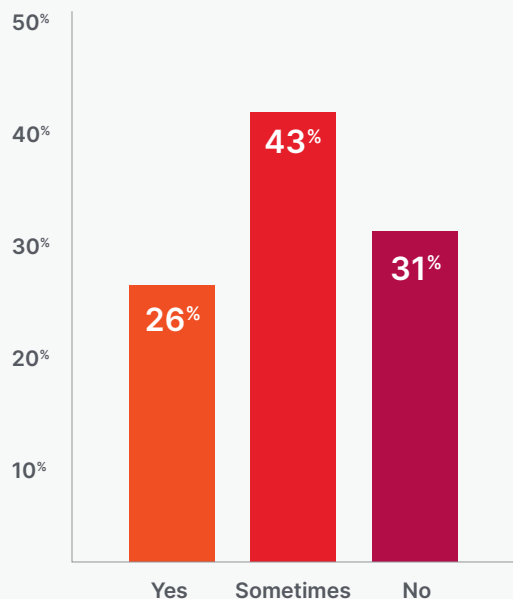
- De nombreux processus sont manuels, sans la cohérence des workflows ou normes IT.
- L'état et l'impact des biens ne sont pas aussi visibles qu'il le faudrait, si bien que les capacités de reporting sont minimales, voire nulles.
- Les coûts et les risques quotidiens sont élevés, les délais rallongent et la qualité de service est médiocre.

La Direction n'est pas toujours au courant de l'impact de l'équipe Services et soutient rarement les nouveaux investissements.



**Survey:**  
**The Impact of Aligning It Service  
& Asset Management Processes**

Do your service management processes and request workflows automatically have visibility into asset information and relationships?



Il convient également d'afficher les résultats ci-dessous, tirés de l'enquête ITXM de décembre 2019, révélant si les processus de gestion des services et de workflows des demandes bénéficiaient d'une visibilité automatique sur les données des biens et les relations entre ces biens.

Comme vous le voyez, moins d'un tiers des personnes interrogées disent bénéficier d'une bonne visibilité sur les informations des biens. Les deux tiers restants expliquent n'en bénéficier que partiellement, voire pas du tout.

Selon la même enquête, les professionnels de l'IT s'attendent à obtenir les améliorations suivantes grâce à l'intégration des processus et données de gestion des services IT et de gestion des biens IT :

- Meilleure visibilité du parc IT : 63 %
- Augmentation de la productivité du personnel IT : 59 %
- Optimisation des coûts : 54 %
- Amélioration de la fourniture de services : 53 %



# 5

## Verrouillage d'un ordinateur portable

Un représentant commercial appelle le centre de support pour signaler que son ordinateur portable est verrouillé (il ne peut plus y accéder) et qu'un message à l'écran demande d'appeler un autre numéro pour le déverrouiller. Il explique aussi qu'il a cliqué sur un lien dans un e-mail parce qu'il pensait qu'il provenait d'un partenaire avec qui il avait travaillé par le passé, et que c'est à ce moment-là que l'ordinateur portable s'est verrouillé. On n'en est pas sûr, mais d'autres collaborateurs ont peut-être reçu le même e-mail.

Dans ce scénario, les difficultés potentielles liées au manque de visibilité sont les suivantes : on ignore le nombre des collaborateurs qui ont reçu le même e-mail, on ne dispose d'aucune vue à jour sur la couverture actuelle des correctifs, on ne sait pas quels sont les collaborateurs qui disposent de privilèges

d'administration sur les machines, enfin, on ne dispose pas d'informations sur le nombre des périphériques infectés et leur état.

En 2019, une enquête sur Windows 10 sponsorisée par Ivanti a montré que la principale inquiétude des personnes interrogées porte sur les fuites de données (41 %), suivi de la crainte des ransomwares/malwares (20 %). En outre, une autre enquête mandatée par Ivanti en avril 2019 a montré que 70 % des entreprises auraient pour priorité la connaissance de l'état de leur sécurité, si elles disposaient d'informations en temps réel. Et près de 60 % voudraient avoir une bonne visibilité des données liées aux applications.

D'un point de vue de gestion unifiée du poste client (UEM), le manque de visibilité augmente le temps nécessaire pour gérer les incidents de sécurité. Cela renforce également le risque de voir un incident se transformer en fuite qui met en danger les données de l'entreprise, alourdit la tâche des équipes déjà surchargées et nuit à la confiance témoignée à l'entreprise. Il peut s'agir des conséquences d'une visibilité limitée ou d'un manque d'intégration des données, qui engendrent des conflits des données des biens ou des informations de sécurité. Cela provoque des failles de sécurité et il devient difficile de réagir rapidement.

A l'inverse, avec une bonne visibilité sur des données précises concernant les correctifs et des informations sur les accès utilisateur, il est possible de réagir plus rapidement aux attaques, de protéger le réseau, de bloquer des menaces comme les ransomwares, d'empêcher leur propagation et de se préparer aux futures attaques.

Le manque de visibilité rend également difficile la réponse efficace aux besoins d'application d'une nouvelle image pour corriger les problèmes décrits plus haut.

Pour un analyste du centre de support, la visibilité complète des biens qui existent dans l'environnement, de l'endroit où ils se trouvent et de la façon dont ils sont utilisés (le tout, sans feuilles de calcul lourdes à gérer) est essentielle pour travailler efficacement, avec des délais de résolution plus courts pour les incidents et les problèmes. Dans ce scénario, en augmentant le champ d'action de visibilité des menaces potentielles provoquées par l'e-mail suspect, l'on accélère la résolution du problème.

# 6

## Un univers IT inconnu

Une analyste IT évalue la sécurité de l'environnement et elle s'aperçoit qu'elle ne connaît pas les machines présentes dans cet environnement, et ne sait pas si elles sont correctement gérées. Seul 75 % de l'environnement est identifié. Au fil des renouvellements notamment, certaines machines ne sont plus gérées. Côté serveurs, des machines virtuelles ont été créées sans les informations de configuration appropriées et n'ont pas été mises à jour avec les correctifs les plus récents.

Dans ce scénario, on ne dispose d'aucune visibilité sur les postes client et les serveurs de l'environnement, et, par conséquent, d'aucune information sur les éléments auxquels des correctifs ont été appliqués dans l'environnement de production. Savoir à tout moment où se trouvent tous les biens d'une entreprise (physiques ou virtuels) est non seulement indispensable pour les services et le support, mais également pour la sécurité. Les biens non gérés et

sans correctifs mettent en danger l'intégrité et la conformité des données. Avec la multiplication des vulnérabilités IT, il devient essentiel d'effectuer le suivi de tous les périphériques.

Le livre blanc EY cité plus haut (« Data Validation the Best Practice for Data Quality in Fixed Asset Management » indique que 30 % des biens fixes IT sont des biens « fantômes » qui sont introuvables. La visibilité des biens est une étape indispensable, parce que de nombreuses entreprises sous-estiment ce qu'elles possèdent. Lorsqu'une entreprise début dans la gestion des biens IT (ITAM), il n'est pas rare de constater qu'elle possède 20 ou 30 % plus de périphériques qu'elle ne le pensait. Vous ne pouvez pas gérer ce que vous ignorez posséder et cela représente un vrai risque pour la sécurité.



Avec les solutions de gestion unifiée du poste client (UEM), vous disposez d'une visibilité et d'un contrôle complets de vos postes clients, ce qui vous aide à tout sécuriser et à éviter les menaces qui découlent des périphériques non protégés et non gérés. Les équipes IT bénéficient d'une stratégie de provisioning automatisé, qui effectue des analyses en temps réel, et réconcilie les informations relatives aux utilisateurs et à leur emplacement. Pour éviter la prolifération des serveurs virtuels, il est essentiel de savoir qui détient des privilèges d'administration, afin que les autres groupes IT puissent uniquement générer des machines virtuelles dotées des mesures de sécurité en vigueur dans l'environnement de production. La capacité à trouver ces nouveaux serveurs et à les ajouter à des groupes permet d'éviter de rater le prochain créneau de maintenance.

De plus, il est essentiel de gérer les biens tout au long de leur cycle de vie. En suivant les données de performances, les problèmes, les mesures correctives, les informations de correctif, les contrats et les licences des biens, vous vous assurez que vos investissements en logiciels et en matériel ont des performances optimales, et qu'ils ne nuisent pas à la productivité des collaborateurs.

## Ivanti : Pour avoir des yeux derrière la tête

Les directeurs IT, les RSSI et les vice-présidents IT n'atteignent pas ces niveaux hiérarchiques et de responsabilité en étant cycloptiques ou myopes. C'est pourquoi la visibilité accrue que vous apportent nos solutions Unified Endpoint Management et Enterprise Service Management, peut compléter et soutenir les objectifs de vos équipes, les données de votre secteur d'activité ainsi que la mission et la vision de votre entreprise.

Découvrez par vous-même comment Ivanti améliore votre visibilité IT, vous permettant d'agir pour réellement améliorer l'expérience IT de vos utilisateurs et de réaliser de vrais gains d'efficacité opérationnelle et de productivité. Contactez-nous pour en savoir plus.

The Ivanti logo consists of the word "ivanti" in a bold, lowercase, sans-serif font. The letter "i" is red, while the remaining letters "vanti" are black. A small registered trademark symbol (®) is located at the top right of the letter "i".

**ivanti**

A vertical decorative bar on the right side of the page, transitioning from red at the top to orange at the bottom.

[ivanti.fr](https://www.ivanti.fr)

[contact@ivanti.fr](mailto:contact@ivanti.fr)