ivanti

Le guide ultime de la gestion unifiée des terminaux

Comment les solutions modernes de gestion des terminaux impactent la sécurité et l'expérience des employés

Au sommaire

ivanti

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 www.ivanti.fr

01

La nouvelle norme pour la gestion post-pandémique des terminaux

Il y a cinq ans, la gestion et la sécurité des terminaux étaient relativement simples.

Les terminaux utilisés dans le cadre des activités de l'entreprise étaient généralement situés au bureau (un environnement contrôlable, dans lequel les terminaux étaient facilement localisables, et étaient gérés par des équipes IT et sécurité travaillant sur site).

Puis, la pandémie de Covid-19 a bouleversé le mode de fonctionnement des bureaux sur site.

Les ordinateurs portables et les appareils mobiles de l'entreprise fonctionnaient sur des réseaux Wi-Fi gérés avant que l'année 2020 ne les oblige à un éloignement permanent !

Cependant, les choses ont changé dans le monde entier au moment du confinement. Du jour au lendemain les équipes IT et de sécurité qui travaillaient auparavant sur site ont dû trouver des solutions dans la précipitation afin de mettre en place le télétravail à partir de la technologie et des périphériques disponibles.

Les exceptions à la règle étaient désormais la règle pour tout le monde.

Aujourd'hui, avec le déclin de la menace mondiale que représente la Covid-19, de nombreux employeurs encouragent leurs employés à revenir au bureau et au statu-quo technologique précédent. Une étude d'Ivanti a révélé que si seulement 13 % des travailleurs intellectuels préfèrent travailler uniquement au bureau, 56 % des chefs d'entreprise estiment que les employés doivent être au bureau pour être productifs. (Ivanti)

Cet écart entre le mode de travail souhaité par les employés et celui que leurs responsables jugent efficace, a placé les équipes IT et sécurité dans une position extrêmement inconfortable, voire insoutenable.

Cette tension est d'autant plus vive qu'un retour complet à la gestion sur site et aux réseaux cloisonnés de 2019 semble à la fois improbable et peu judicieux :

> Selon une enquête réalisée en 2022 par le site mondial d'offres d'emploi Monster.com, deux tiers des employés préfèrent démissionner plutôt que de retourner au bureau pour une semaine de travail complète, et 40 % des personnes interrogées ont affirmé pour leur part être prêtes à démissionner si leur retour au bureau leur était imposé pour seulement un jour de travail sur cinq au cours d'une semaine de travail. (Shumway)

> Dans un ultimatum datant de novembre 2022, le PDG de Twitter, Elon Musk, a exigé un retour des employés à leur bureau local 40 heures par semaine ou bien leur démission. (Yang) Des centaines de salariés l'ont pris au mot et ont démissionné. (Bond) Début janvier 2023, le nombre d'employés à temps plein de Twitter a diminué de plus de 80 %, passant d'environ 7 500 employés à environ 1 300, avec moins de 550 ingénieurs à temps plein. (Kolodny)

> Lorsque le PDG d'Amazon, Andy Jassy, a ordonné à ses collaborateurs technologiques de retourner au bureau à temps plein en février 2023, ils ont refusé. Finalement, il a cédé, déclarant qu'ils ne devaient être au bureau que trois jours par semaine. (Palmer)

Pour ceux ayant la conviction que le retour au bureau améliorera la productivité, les recherches démontrent le contraire :

- Pendant la pandémie, Gallup a enregistré un taux d'engagement des employés de 40 %, le plus élevé de son histoire ; depuis, ce taux a chuté à moins d'un tiers. (Smith)
- Le premier semestre 2022 montre un « effondrement » record de la productivité au cours du premier semestre 2022, en corrélation avec la pression accrue des organisations exigeant de tous les employés leur retour au bureau à temps plein. (Tsipursky)

Ces tendances nous indiquent que malgré le retour au bureau imposé par les organisations, les employés démissionnent discrètement : certains font le strict minimum tout en recherchant de nouvelles opportunités leur permettant de bénéficier des modalités de travail flexibles si attrayantes obtenues au moment du confinement. (Tsipursky)

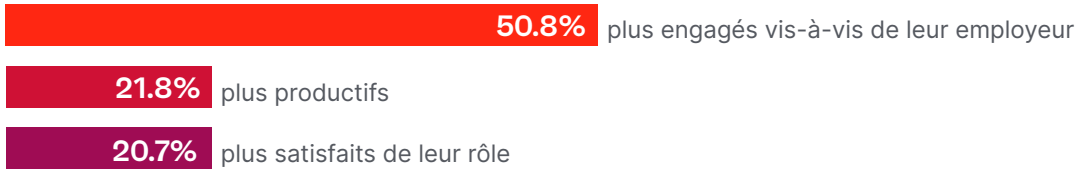
La solution évidente ? Encourager les employés à continuer leur travail à distance, sur site ou une combinaison qui convient le mieux à chaque collaborateur, chaque fois que c'est possible.

En effet, les employés qui travaillent dans un environnement hybride ou à distance déclarent être 21,8 % plus productifs, 20,7 % plus satisfaits et 50,8 % plus engagés, comme l'indique une enquête de l'Integrated Benefits Institute réalisée en 2022. (Bonner)

Bien entendu, cette nouvelle exigence présente de nouveaux défis pour les équipes informatiques et de sécurité ; et c'est là que les solutions de gestion unifiée des terminaux peuvent vous aider.

Malgré cela, si votre organisation décide de travailler dans un environnement exclusivement sur site, sans envisager aucunement le travail à distance - ou bien souhaite tendre vers cet objectif - vos équipes savent pertinemment qu'une configuration de travail et de sécurité totalement en présentiel ne fonctionnera pas car il faut tenir compte des « exceptions », comme nous l'expliquons dans ce guide.

Les employés qui travaillent dans un environnement hybride ou à distance sont :



Les « exceptions » hybrides et à distance à la règle du travail 100 % en présentiel

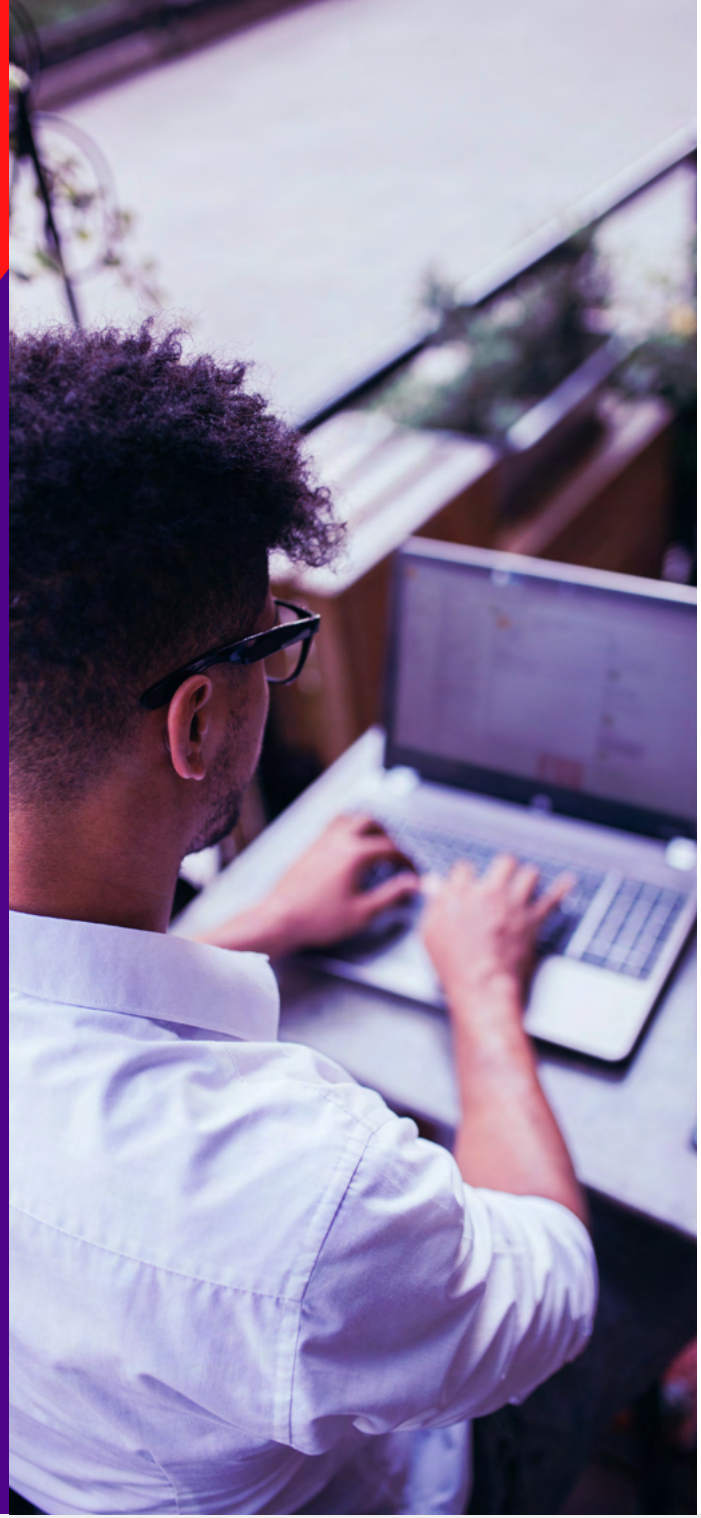
Votre organisation peut envisager de travailler entièrement « au bureau » et donc nécessiter uniquement les solutions traditionnelles de gestion et de sécurité des terminaux utilisées avant la pandémie, mais le travail s'effectue-t-il réellement sur place à 100 % ?

Bien sûr que non !

Les équipes IT et Sécurité doivent anticiper toutes les exceptions aux procédures standard. C'est pourquoi une stratégie hybride de sécurité et de gestion des technologies sera toujours plus robuste qu'une stratégie qui part du postulat que seuls les environnements de travail devant être sécurisés et gérés sont ceux sur site.

Ainsi, les stratégies hybrides de gestion et de sécurité des technologies de l'information couvrent les « exceptions » aux situations exigeant un travail totalement en présentiel :

- **les prestataires de soins de santé** qui sont de garde le week-end nécessitent un accès aux dossiers des patients pour répondre à un appel.
- **les enseignants** qui corrigent des copies à la maison ou répondent aux e-mails des parents après les heures de travail.
- **les conseillers financiers,** qui doivent pouvoir accéder à leurs e-mails uniquement sur un serveur sécurisé… mais qui ont peut-être installé une application leur permettant d'y accéder par leurs appareils personnels.
- **les parents** qui tentent de travailler à domicile tout en s'occupant d'un enfant malade.
- **des fonctionnaires** qui assistent à des conférences ou voyagent pour remédier à des incidents, mais ont toujours besoin d'un accès aux réseaux de leur bureau depuis leur domicile.
- **des cadres supérieurs** cherchant à obtenir des dérogations pour des raisons de commodité liées à leur ancienneté.
- **des commerciaux.**



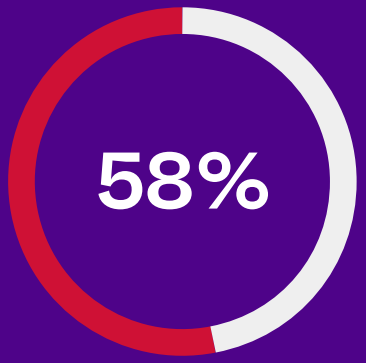
Même si pour la plupart des utilisateurs finaux le lieu de travail est redevenu le bureau de l'entreprise, ils souhaitent pouvoir se connecter à distance aux données et applications professionnelles depuis leurs appareils mobiles ou via n'importe quel réseau accessible depuis leur Bluetooth.

Les équipes informatiques et de sécurité doivent donc adapter des stratégies permettant aux employés de travailler au bureau et en dehors, et ce, en maîtrisant de manière efficace les périphériques et les réseaux. Cela signifie sécuriser tous les terminaux et leurs utilisateurs finaux, quels que soient l'endroit et le réseau, et ce pour toutes les données de l'organisation.

Mais cette nouvelle obligation de gérer et sécuriser les terminaux dans un environnement de travail hybride de facto, indépendamment du statut officiel de retour au bureau, ne contraint pas les organisations à s'appuyer sur ces mêmes stratégies de panique employées il y a quelques années pour gérer les périphériques en cas de pandémie.

Ces solutions d'urgence ont fonctionné pendant un certain temps, mais elles sont insuffisantes pour gérer les terminaux à long terme et les protéger des risques et des vulnérabilités modernes, accentuant la nécessité pour les entreprises de disposer d'une solution de gestion des terminaux parfaitement unifiée.

En effet, 58 % des RSSI déclarent que leur entreprise a subi davantage de cyberattaques depuis le passage au travail à distance. (Proofpoint)



des RSSI déclarent que leur entreprise a subi davantage de cyberattaques depuis qu'elle autorise ses employés à travailler à distance

ivanti

02

Qu’est-ce que la gestion unifiée des terminaux ?

La gestion unifiée des terminaux (UEM) désigne une technologie offrant aux équipes informatiques et de sécurité la possibilité de trouver, gérer et sécuriser plusieurs terminaux, c’est-à-dire des périphériques, du matériel et d’autres technologies, à partir d’une seule plateforme ou d’un seul tableau de bord, couvrant ainsi un large éventail de systèmes d’exploitation (OS) et types de périphériques provenant de nombreux fabricants et développeurs différents.

L’UEM représente la dernière évolution des solutions de gestion des terminaux, issues des premières technologies de gestion des périphériques mobiles (MDM).

- **La gestion des périphériques mobiles (MDM),** souvent rebaptisée aujourd’hui gestion « moderne » des périphériques, constitue la première tentative de l’industrie technologique visant à résoudre les problèmes de gestion, application et sécurité liés à l’augmentation constante des flottes d’appareils. Ces solutions permettaient aux services informatiques de contrôler, sécuriser et appliquer des politiques, des configurations et des logiciels sur les smartphones, tablettes et autres terminaux prenant en charge les API MDM, mais elles étaient souvent limitées aux appareils fonctionnant sous des systèmes d’exploitation spécifiques.

- **La gestion mobile d’entreprise (EMM)** a repris la technologie MDM et l’a fusionnée avec des solutions de gestion des applications logicielles telles que la gestion des applications mobiles (MAM), la gestion du contenu mobile (MCM) et la gestion de l’information mobile (MIM) pour gérer à la fois le cycle de vie des logiciels sur le périphérique, les données sur des applications spécifiques et l’accès aux données de l’entreprise.

Cependant, l'approche mixte de la gestion des terminaux était encore insuffisante pour prendre en compte les ordinateurs personnels traditionnels, les serveurs et autres terminaux d'entreprise classiques, ainsi que de nombreux cas d'utilisation marginale en pleine croissance dans les environnements d'organisation modernes, y compris les appareils IoT et les équipements plus « robustes » ou spécialisés rencontrés dans des situations de travail spécifiques, mais courantes.

Les équipes informatiques des grandes organisations se sont retrouvées dans un système de patchwork pour gérer plusieurs OS : macOS, Windows, iOS et Android, mais aussi ChromeOS, Linux et d'autres appareils spécialisés ou compatibles avec l'IoT.

Bien que chaque fournisseur d'OS prenne en charge les commandes et les configurations via leur MDM natif, plusieurs tâches critiques ne sont pas incluses dans les API MDM :

- statut de l'appareil (jailbreak, détection de la racine)
- emplacement
- notifications
- défense contre les menaces mobiles

La technologie de gestion unifiée des terminaux est donc née de la nécessité pour les entreprises de fournir des capacités supplémentaires et des contrôles d'application tout en les étendant à plusieurs types de systèmes d'exploitation et appareils, à la fois dans la gestion des terminaux mobiles et traditionnels.

03

4 avantages métier d'une solution UEM moderne

Dans cette section, découvrez comment l'UEM :

1. consolide les piles technologiques,

2. découvre automatiquement les actifs inconnus,

3. améliore la conformité des utilisateurs,

4. améliore l'expérience numérique des employés (DEX).

ivanti

La différence UEM

Aujourd'hui, la plupart des entreprises appliquent déjà au minimum une solution pour gérer l'ensemble des périphériques leur appartenant et sous leur gestion.

Une enquête réalisée en 2022 auprès de professionnels de l'informatique a révélé que 80 % des personnes interrogées avaient déjà consolidé leur équipe de gestion des terminaux ou l'envisageaient dans les deux années à venir. Et 75 % des personnes interrogées ont investi dans une forme de technologie d'activation BYOD (bring your own device). (Cipolla, Wilson et Silva)

Au lieu de fonctionner en silos au niveau des périphériques, les solutions UEM utilisent mieux les capacités modernes d'IA et d'apprentissage automatique (ML), puisque ces outils exploitent le même ensemble de base d'informations à l'échelle de l'organisation pour tirer des conclusions, plutôt que de s'appuyer sur des flux d'informations cloisonnés provenant d'outils distincts.

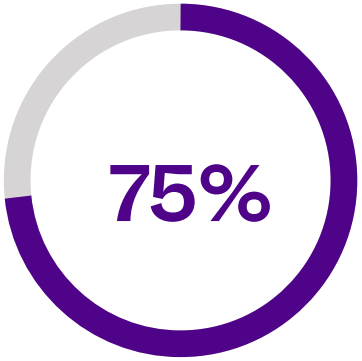
Les avantages d'une solution UEM moderne :

1. **Des tableaux de bord ou des portails à « écran unique »,** offrant aux équipes informatiques et de sécurité déjà très réduites une solution consolidée au lieu de plusieurs produits de niche.

2. **L'identification automatique et la remédiation des dispositifs inconnus** et de ce que l'on appelle le « shadow IT » grâce à la découverte dynamique et automatique des actifs, à la fois sur site et via le Cloud.

3. **La conformité accrue de l'utilisateur final** avec toutes les politiques informatiques et de sécurité par le biais d'un enrôlement et d'une mise en œuvre unifiées des périphériques.

4. **L'amélioration de l'expérience numérique des employés (DEX)** grâce à la résolution automatique et proactive des problèmes liés aux périphériques, afin de permettre un « shift left » aux équipes informatiques concernées.



des professionnels de l'informatique déclarent que leur organisation a investi dans la mise en œuvre du BYOD.

1 Une approche de type « écran unique » consolide les empilements technologiques fastidieux.

Dans un contexte d'incertitude économique croissante, les investisseurs et les chefs d'entreprise demandent à leurs organisations d'optimiser les résultats stratégiques en investissant moins de ressources, en maximisant l'efficacité et en tirant le maximum de valeur de chaque outil, de chaque employé et de chaque délai.

Dans le cadre de ce processus, les organisations se tournent de plus en plus vers l'achat de solutions technologiques plus généralisées et intégrées, au lieu de rechercher des solutions ponctuelles impliquant plus de main-d'œuvre et des connaissances spécialisées dépassant la capacité de prise en charge de leurs équipes informatiques et de sécurité.

Cette évolution stratégique vers la consolidation de la pile technologique semble logique, surtout au regard des tendances mondiales en matière d'épuisement professionnel et de main-d'œuvre technologique :

- 64,4 % des employés des services d'information interrogés dans le cadre d'une enquête mondiale réalisée en 2019 ont fait état d'un épuisement professionnel, soit l'un des taux les plus élevés de tous les secteurs d'activité. Les employés du secteur général de la « technologie » ont également signalé des niveaux élevés d'épuisement professionnel avec un taux de réponse de 60 %. (Paychex)
- 68 % des personnes interrogées sur les incidents déclarent se voir généralement confier deux incidents ou plus à la fois, chaque incident nécessitant en moyenne deux à quatre semaines pour être résolu ; 64 % de ces mêmes personnes ont également demandé une aide médicale pour traiter l'épuisement et l'anxiété. (Morning Consult et IBM)
- Le principal obstacle à l'excellence en matière de cybersécurité pour les organisations du monde entier réside dans la « complexité de la pile technologique », suivie par le « déficit de compétences en matière de sécurité » du personnel de sécurité actuel, selon une enquête mondiale réalisée en 2022 auprès de professionnels de la sécurité. (Ivanti)

Comme l'a déclaré un RSSI au Wall Street Journal :

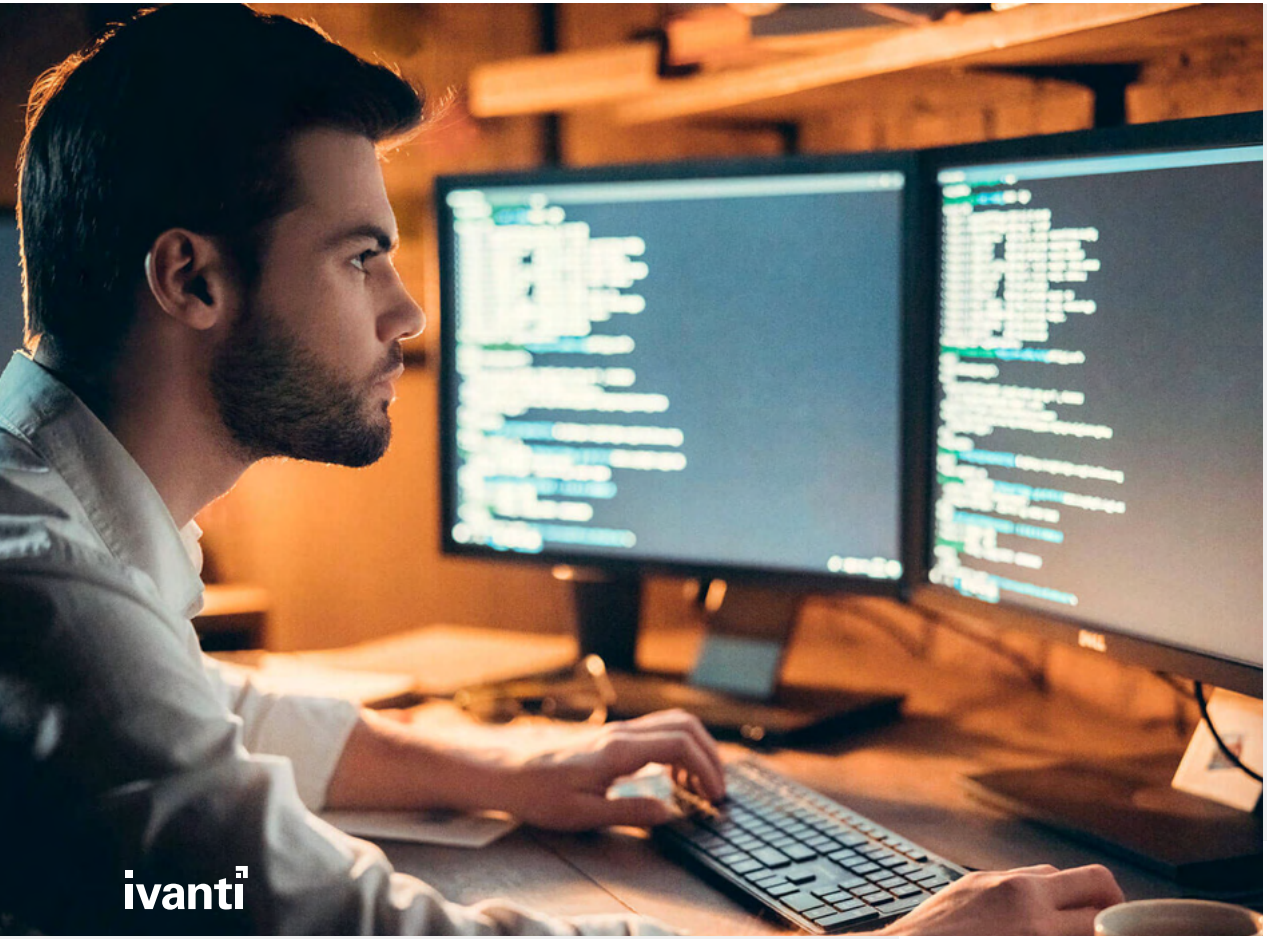
« Si je dois opter pour une solution capable d'accomplir cinq ou six tâches assez bien, mais pas de manière excellente, alors parfait, j'opte tout de suite pour cette solution. C'est plus facile à gérer, ça pèse moins sur le budget, et j'en ai plus pour mon argent. »

Adam Glick
CISO chez SimpliSafe, Inc. (Rundle)

Qu'est-ce que cela signifie ? Sur le marché de l'emploi et dans l'entreprise, peu de personnes disposent des compétences requises pour gérer chaque appareil, application et incident à mesure qu'ils apparaissent sur des solutions déconnectées.

Correctement configurées et mises en œuvre, les plateformes UEM modernes offrent aux équipes informatiques et de sécurité une seule et même interface de l'ensemble de l'environnement des terminaux de l'entreprise, avec des rapports dynamiques sur :

- l'utilisation et la gestion des appareils au niveau du département et de l'utilisateur,
- l'accès et l'activité des utilisateurs individuels, afin d'évaluer la productivité globale et les problèmes de sécurité potentiels,
- l'état de sécurité d'un terminal, y compris les correctifs installés et les cas d'utilisation,
- le coût global d'un dispositif pour les opérations, en tenant compte de l'historique des coûts de maintenance et de licence.



Chacun de ces points peut être pris en charge par des solutions ponctuelles pour un type de périphérique ou un système d'exploitation donné, avec des niveaux de granularité et de détail encore plus élevés pour les opérations les plus optimisées.

Cependant, seule une solution UEM moderne peut réellement unifier ces besoins connexes mais distincts en un tableau de bord unique et simple à gérer, permettant aux équipes informatiques et de sécurité surchargées de l'exploiter dans le cadre de leurs flux de travail personnels.

2 La détection automatisée des actifs permet de déterminer les coûts cachés avec un minimum de main-d'œuvre.

Tout comme l'utilisation de plusieurs solutions technologiques pour gérer les terminaux augmente les dépenses globales, une détection insuffisante des actifs peut entraîner une augmentation des frais généraux et des coûts pour les organisations ; des coûts que l'équipe informatique devra finalement assumer, peu importe la source des fuites.

Les équipes informatiques sont de plus en plus conscientes du danger que représentent les matériels et logiciels non détectés (et donc non gérés), plus communément appelés Shadow IT :

- 36 % des professionnels de l'informatique citent les problèmes liés au shadow IT comme un défi majeur dans la modernisation de leur infrastructure informatique. (Insight Enterprises & CIO)
- Le Shadow IT constitue l'une des principales préoccupations citées par les DSI interrogés pour la continuité de l'administration, après les attaques par ransomware et les attaques de la chaîne d'approvisionnement. (NASCIO)
- 41 % des responsables informatiques interrogés déclarent que l'informatique « décentralisée » et le Shadow IT représentent l'une des plus grandes tendances susceptibles d'impacter les organisations mondiales dans un avenir proche. (Vanson Bourne pour Nutanix)

Pourquoi les considérations relatives au Shadow IT sont-elles devenues une priorité au sein des départements informatiques ? La multiplication des lieux de travail hybrides et des politiques BYOD (bring your own device) s'accompagne de l'augmentation du nombre de périphériques et d'applications utilisés par les utilisateurs finaux, mais sans nécessairement être directement détenus ou gérés par l'équipe informatique elle-même.

Selon une enquête menée auprès des responsables informatiques (Bitwarden), les utilisateurs finaux déclarent avoir recours au Shadow IT pour les raisons suivantes :

1. leur travail quotidien est plus rapide ou plus facile avec les options de Shadow IT de leur choix, plutôt qu'avec les ressources fournies par l'organisation (63%) ;

2. ils n'ont pas les autorisations internes nécessaires pour utiliser les périphériques ou les applications indispensables à leur activité (48 %) ;

3. le département informatique répond trop lentement à leurs demandes d'accès aux applications ou aux périphériques, ou ils choisissent de ne pas le contacter car c'est trop compliqué (38 %).

Répercussions dans le monde réel

Consolidation des technologies et des licences grâce à l'UEM

Selon une étude Total Economic ImpactTM réalisée par Forrester Consulting pour le compte d'Ivanti, une entreprise de taille moyenne gérant 10 000 terminaux et enregistrant une croissance annuelle de 5 % a obtenu un retour sur investissement de 261 % sur trois ans en mettant en œuvre Ivanti Neurons pour UEM.

36 % des bénéfices estimés par l'étude TEI pour l'organisation composite proviennent du retrait des solutions individuelles de gestion des terminaux et de la réduction des dépenses de licences logicielles pour les applications inutilisées. (Étude TEI de Forrester Consulting)

Pour plus d'informations, veuillez lire l'impact économique total™ des solutions de gestion unifiée des terminaux (UEM) d'Ivanti.

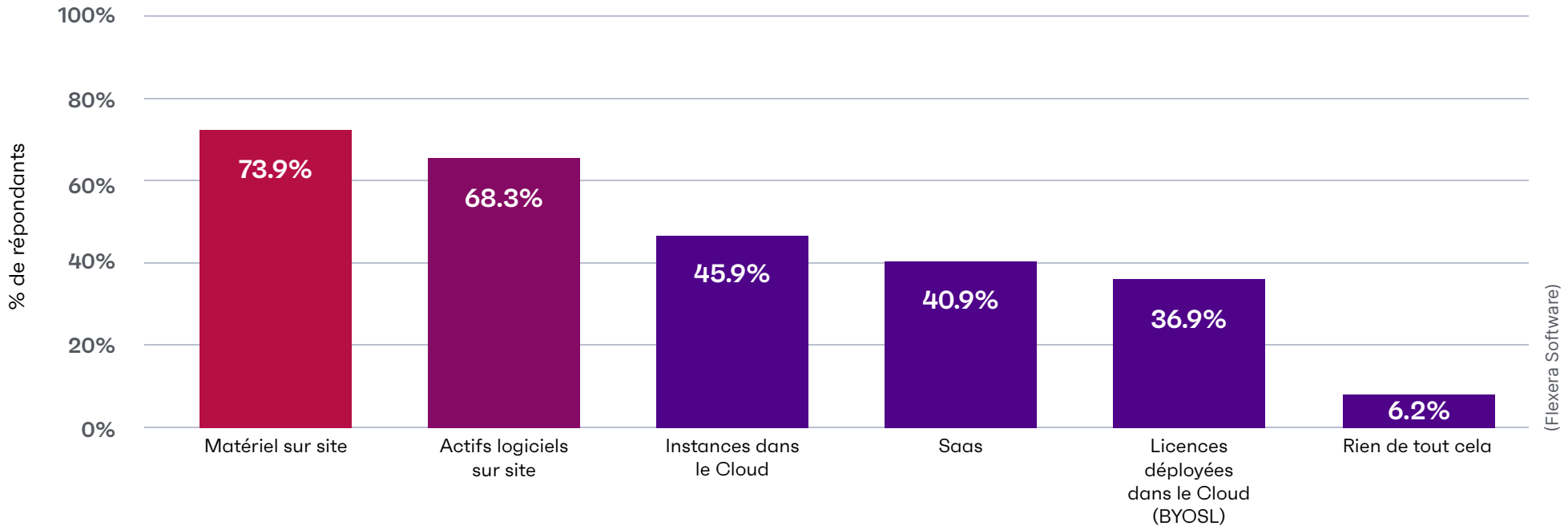
Autre facteur contribuant aux problèmes de Shadow IT : les équipes IT maîtrisent mieux la visibilité des actifs déployés sur site que celle des actifs déployés à distance ou dans le Cloud. (Flexera Software)

Ces enquêtes et études mondiales sont en corrélation avec l'expérience anecdotique d'Ivanti auprès de ses clients, qui constatent que 25 à 30 % d'appareils jusque-là inconnus accèdent aux réseaux de l'entreprise après le déploiement d'une solution UEM dotée de capacités de détection active des actifs.

La détection automatisée des actifs via une plateforme UEM centralisée permet aux équipes informatiques de :

- détecter tous les appareils dès leur connexion à l'infrastructure et aux réseaux de l'entreprise ;
- réduire le risque de voir des appareils transitoires en ligne sans remédiation ni segmentation ;
- analyser les appareils à distance sans agent ;
- segmenter et mettre en quarantaine les appareils inconnus potentiellement dangereux, tout en conservant la flexibilité d'une politique BYOD.

Q: Pensez-vous disposer d'une visibilité précise sur les environnements suivants ?



3 L’enrôlement automatique du périphérique accélère l’onboarding et la conformité de l’utilisateur final.

Une partie de la stratégie de travail hybride de facto implique la prise en charge de l’intégration initiale des nouveaux employés, y compris le provisionnement de nouveaux appareils avec les logiciels et les autorisations d’accès appropriés pour les utilisateurs finaux qui ne mettront peut-être jamais les pieds au bureau !

Les solutions UEM offrent des profils d’utilisateurs et d’appareils préconfigurés pour rendre les déploiements les plus simples possibles : il suffit par exemple au responsable du recrutement d’accéder à un portail en libre-service pour procéder aux demandes et autorisations, sans solliciter l’équipe IT.

Grâce à un enrôlement automatisé des terminaux, de nouveaux appareils et profils d’utilisateurs peuvent être ajoutés en interrompant le moins possible les tâches régulières de l’équipe informatique ou les flux de travail ordinaires des employés.

L’application automatique des politiques et des configurations de dispositifs à partir de la solution UEM principale garantit également la conformité universelle des politiques.

Enfin, en déployant une solution UEM, les entreprises ne sont plus obligées de compter sur les utilisateurs finaux pour obtenir les mises à jour ou les applications de sécurité nécessaires. Les appareils gérés par l’UEM sont automatiquement enrôlés dans le calendrier de mise à jour spécifique ou dans l’installation de l’application ; aucune interaction ou autorisation de l’utilisateur n’est requise !

Répercussions dans le monde réel

De 2 à 3 jours à 5 à 10 minutes pour installer et configurer des logiciels

Au cours des entretiens réalisés dans le cadre d’une étude TEI commandée par Forrester Consulting pour le compte d’Ivanti, un ingénieur en intégration d’un détaillant de chaussures a estimé la durée d’installation et de configuration des logiciels de son équipe à deux ou trois jours par périphérique. (Étude TEI de Forrester Consulting)

Après avoir mis en œuvre Ivanti Neurons for UEM, la personne interrogée a toutefois déclaré : « Désormais, une fois l’image obtenue, il suffit d’installer Ivanti puis de déplacer le périphérique par un simple glisser-déposer dans les tâches exécutées par le logiciel. Le processus dure de cinq à dix minutes, et il suffit ensuite de le vérifier à la fin de la journée pour s’assurer de la présence de toutes les applications. Cela nous a permis de gagner du temps dans le processus d’intégration de l’utilisateur. » (Étude TEI de Forrester Consulting)

FORRESTER®

4 Les utilisateurs finaux font état d'une expérience numérique optimisée et d'une productivité accrue.

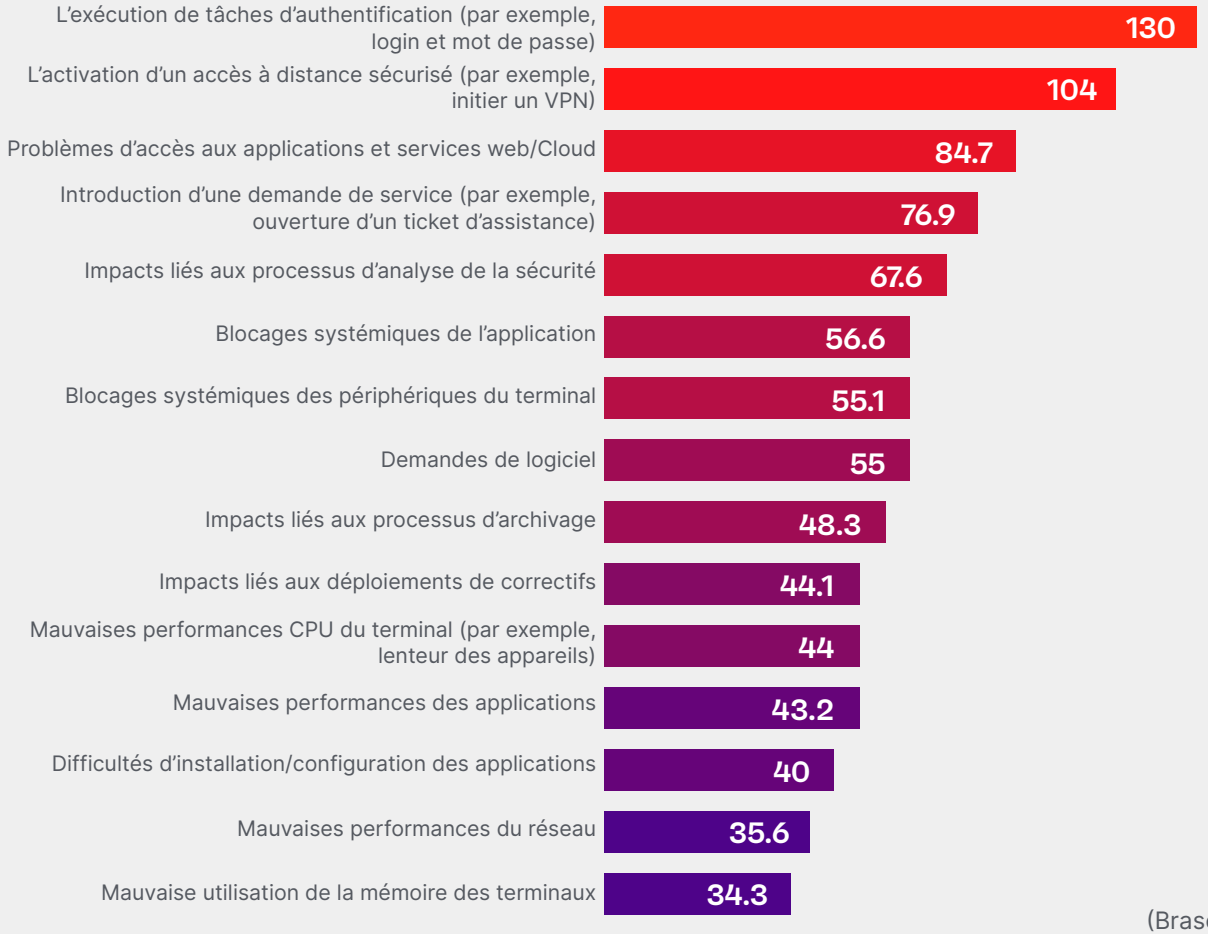
Toutes les équipes informatiques et de sécurité seront d'accord avec ce simple fait : l'expérience numérique des employés (DEX) est essentielle.

Des recherches récentes sur l'expérience numérique des employés confirment cette vérité presque instinctive :

- 26 % des salariés interrogés, et 31 % des professionnels de l'informatique et de la sécurité, ont envisagé de quitter leur emploi, au moins en partie, en raison de difficultés liées à la technologie. (Ivanti)
- Chaque année, un employé moyen est confronté à 919 problèmes de gestion des terminaux, ce qui équivaut à près de quatre problèmes par jour ouvrable. (Brasen)
- Un utilisateur nécessite jusqu'à 20 minutes pour résoudre chaque interruption causée par une mauvaise gestion des terminaux et des problèmes technologiques. (Brasen)

En effet, la DEX est si importante que les analystes de Gartner prévoient d'ici 2025 la mise en place d'une stratégie, d'une équipe et d'une gestion de la DEX dans 50 % des organisations informatiques, contre seulement 15 % en 2022. (Wilson, Cipolla et Paulman)

Nombre moyen de fois par an où chaque utilisateur rencontre des problèmes liés à l'expérience numérique, selon les entreprises interrogées



(Brasen)

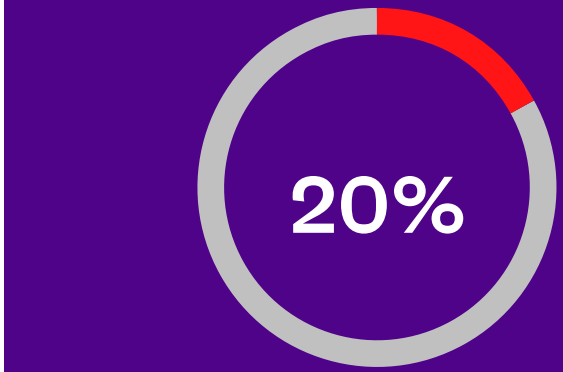
Bien entendu, la mise en œuvre d'une stratégie DEX appropriée est un défi dans presque toutes les situations. Cependant, cela devient particulièrement difficile lorsque seulement 20 % des dirigeants interrogés prévoient d'allouer des budgets pour améliorer l'expérience de leurs employés au cours de l'année à venir. (Ivanti)

Cependant, les solutions UEM peuvent donner aux équipes informatiques une vue d'ensemble rapide des périphériques et des activités de l'utilisateur, permettant aux techniciens d'évaluer les problèmes en un clin d'œil ou bien d'approfondir les analyses afin de déterminer la cause première des frustrations de l'utilisateur et accélérer ainsi la résolution des problèmes.

Les solutions UEM modernes - avec des alertes personnalisées sur l'activité des périphériques et des utilisateurs, ainsi que des accords de niveau de service préprogrammés et des plans d'action - peuvent en outre détecter automatiquement et résoudre de manière proactive un grand nombre de ces problèmes technologiques de gestion médiocre des terminaux.

Ainsi, des solutions UEM fiables et correctement configurées représentent l'un des aspects les plus fondamentaux et cruciaux d'une stratégie DEX solide, permettant un « shift left » aux équipes informatiques en charge de la gestion des services pour remédier aux problèmes liés aux terminaux avant que les utilisateurs ne soumettent un ticket d'assistance.

Toutes les équipes informatiques et de sécurité peuvent économiser du temps et de l'argent grâce à des plateformes technologiques proactives telles que les solutions UEM - et ce, malgré un manque de compréhension de la part des dirigeants quant à l'importance des investissements dans la DEX.



Seuls 20 % des dirigeants prévoient d'allouer des budgets spécifiques à l'amélioration de l'expérience des employés.

ivanti

04

4 cas d'utilisation des solutions UEM en matière de sécurité des terminaux

Dans cette section, découvrez de quelle manière votre solution UEM aide votre équipe de sécurité à :

1. encourager les bons comportements en matière de sécurité ;

2. sécuriser un environnement de travail hybride en pleine croissance ;

3. appliquer automatiquement les politiques ;

4. s'intégrer facilement aux solutions de correctif ou de défense contre les menaces mobiles.

ivanti

Pourquoi les utilisateurs d'UEM doivent-ils également prendre en compte la sécurité des terminaux

Vous avez peut-être remarqué que nous faisons souvent référence aux équipes informatiques et de sécurité tout au long de ce guide ; et ce n'est pas un hasard.

Compte tenu des approches hybrides et à distance adoptées par la tendance post-pandémique à travailler de partout, plutôt que des bureaux situés uniquement sur site, les analystes tiers pensent que les solutions UEM évolueront pour intégrer davantage de cas d'utilisation visant à défendre proactivement et avec résilience les terminaux contre les « threats actors » modernes. (Cipolla, Wilson et Silva)

Il n'est donc pas surprenant que la sécurité des terminaux reste une priorité d'investissement en matière de cybersécurité pour les organisations du monde entier, devancée seulement par les outils de sécurité Cloud et la formation des utilisateurs internes. (PwC)

(Et si la solution UEM proposée pouvait contribuer à sécuriser les applications Cloud, ce serait un avantage pour toutes les parties concernées !)

Les solutions UEM offrent un point de départ unique aux équipes informatiques et de sécurité pour travailler à partir du même ensemble d'informations de base - les périphériques, les profils d'utilisateur et les activités réseau de leur organisation - afin de gérer, sécuriser et entretenir correctement tous les terminaux.

1. **Investir dans une pile technologique axée sur la DEX** pour inciter les utilisateurs finaux à adopter des comportements adéquats en matière de sécurité.

2. **Sécuriser le champ d'attaque en expansion rapide d'une organisation** signifie pour les équipes de sécurité faire face à une plus grande variété de vecteurs de menaces qu'auparavant, depuis les dispositifs IoT jusqu'aux connexions Internet inconnues.

3. **L'application des politiques de sécurité et la surveillance du comportement des utilisateurs, appareils et applications permettent** de prévenir tout mouvement latéral au sein du réseau de l'organisation à partir d'un terminal compromis, et signaler les intrusions initiales ou les menaces potentielles internes avant tout risque de dommage.

4. **Les outils de sécurité tels que les solutions de défense contre les menaces mobiles et de gestion des correctifs** s'intègrent facilement aux solutions UEM modernes, offrant aux équipes de sécurité une méthode simple et rapide de remédier aux risques prioritaires et ce, sans interférer avec les opérations régulières des utilisateurs ou des administrateurs informatiques.

Toutefois, bien que les automatismes d'intégration des appareils et les contrôles de politique d'UEM offrent certaines protections d'hygiène cybernétique de base - et que les journaux d'activité des appareils et utilisateurs offrent une surveillance efficace prisée des équipes de sécurité - la plupart des plateformes nécessiteront des contrôles et des outils supplémentaires pour atteindre leur plein potentiel en tant que point unique de vérité d'une organisation pour toute la sécurité des terminaux. (Verizon)

1 La sécurité dans UEM commence avec la DEX.

Plus que tout autre département en dehors de l'informatique, les équipes de sécurité soutiendront les investissements en faveur d'une technologie DEX plus proactive, y compris les solutions UEM, d'autant plus que les risques liés au Shadow IT et les surfaces d'attaque des terminaux en constante expansion ne cessent d'augmenter dans un environnement de travail hybride post-pandémie.

- Les responsables informatiques citent les solutions ou les produits liés au shadow IT comme l'une des principales préoccupations en matière de continuité des gouvernements dans le monde. (NASCIO)
- 12,8 % des cyberattaques basées sur l'informatique Cloud en 2022 impliquaient le shadow IT. (Shackleford)
- Seuls 52 % des professionnels de la sécurité interrogés font état d'un degré « élevé » de visibilité des actifs au sein de leur organisation ; et 10 % déclarent n'utiliser aucun outil de détection des actifs. (Ivanti)

Les pirates informatiques profitent déjà de ce fossé entre ce que l'équipe de sécurité pense être en mesure de protéger et ce que les utilisateurs ont mis en place pour faciliter leur travail.

12.80% **de toutes les cyberattaques basées sur le Cloud en 2022 impliquaient le shadow IT.**

Répercussions dans le monde réel

Quand une mauvaise DEX a presque permis à des pirates de faire exploser une usine pétrochimique

En 2017, des acteurs de la menace ont piraté l'usine pétrochimique saoudienne Triconex. L'équipe de sécurité a réalisé que leurs systèmes avaient été violés seulement lorsque six contrôleurs ont mal fonctionné, déclenchant une alarme.

Les intervenants ont rapidement découvert qu'une personne avait accédé à distance aux systèmes pour y insérer un logiciel malveillant, pourtant cela semblait impossible !

Après tout, les systèmes de sécurité de l'usine avaient été conçus pour déjouer les attaques à distance en exigeant qu'un employé insère une clé physique dans la console de l'usine pour effectuer des changements de configuration.

Cependant, l'agencement physique de l'usine séparait le contrôleur de la salle de contrôle, obligeant les opérateurs à faire des allers-retours d'un espace à l'autre pour effectuer des changements. Un employé avait conservé sa clé physique dans la console du contrôleur pour lui permettre, ainsi qu'aux pirates, d'accéder à distance au code et procéder ainsi à des mises à jour.

Si d'autres systèmes de sécurité redondants n'avaient pas alerté les employés de l'usine des défaillances critiques déclenchées par les activités du pirate, les contrôleurs compromis de Triconex auraient pu éteindre tous les systèmes de sécurité et tuer les employés de l'usine, soit par des fuites de produits chimiques, soit par des explosions pures et simples.

Cette cyberattaque aurait pu être l'une des premières à entraîner des pertes humaines ; tout cela en raison d'un employé fatigué et de l'incapacité du concepteur de la sécurité à prendre en compte le comportement humain dans la création d'un système de sécurité « infaillible ». (Rhysider)

2

Sécurisez des environnements de travail plus diversifiés et des terminaux IoT via des clients UEM.

Le travail à distance évoque des images d'employés travaillant dans un café, les écouteurs branchés, ignorant totalement qu'un « client » attend qu'ils se rendent aux toilettes pour télécharger des fichiers exclusifs et exploiter leur ordinateur portable déverrouillé.

Si l'erreur humaine subsistera toujours dans une certaine mesure, les solutions et politiques de sécurité des terminaux, appliquées par la plateforme UEM de l'équipe informatique, contribueront à remédier à certains des risques inhérents à un lieu de travail plus diversifié sur le plan géographique.

Examinons deux des risques les plus courants en matière de sécurité des terminaux : la prolifération de l'Internet des objets (IoT) et les attaques de type « l'homme au milieu » dans les réseaux publics.

(Attention : ces deux scénarios peuvent être corrigés grâce à une détection appropriée des actifs, une segmentation du réseau et une surveillance des appareils ; autant de mesures qui peuvent être exécutées par le biais de solutions UEM dotées des configurations et des fonctions de soutien adéquates, axées sur la sécurité.)

Répercussions dans le monde réel

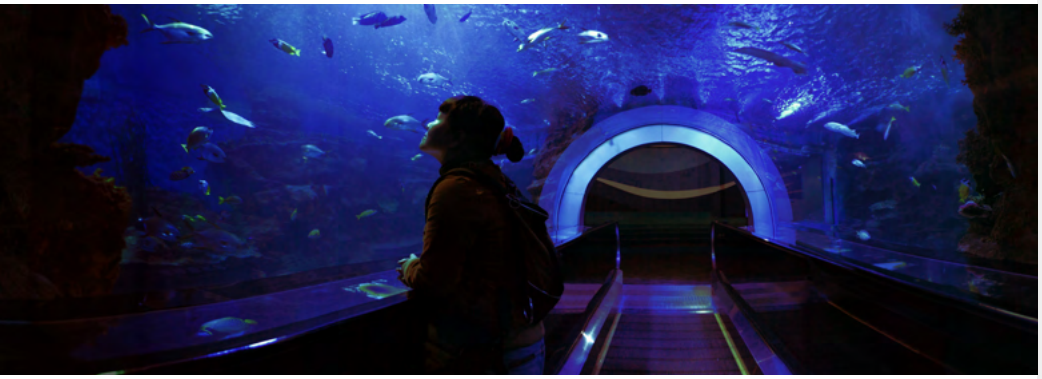
Attaques inattendues de l'Internet des objets (IoT)

Les attaques IoT représentaient plus de 12 % de toutes les attaques mondiales de logiciels malveillants en 2021 - contre moins de 1 % de toutes les attaques de logiciels malveillants en 2019. (Sécurité IBM)

Pourtant, 47 % des professionnels de l'informatique interrogés ont signalé l'absence de politique de conformité à l'IoT au sein de leur organisation. (SAM)

Les appareils compatibles avec l'IoT dans les entreprises et les lieux de travail distants peuvent être remédiés grâce à une segmentation relativement simple du réseau et à des capacités d'analyse active.

Cependant, la plupart de ces appareils sont ceux que les entreprises et les utilisateurs finaux ne prennent pas nécessairement en compte dans leur analyse des risques, jusqu'à ce qu'il soit trop tard, comme l'ont découvert ces entreprises.



Thermomètres de vivier

Un casino nord-américain a découvert les ravages d'un IoT non géré sur ses opérations, lorsque des pirates ont exploité une vulnérabilité dans le thermomètre du vivier de son hall d'entrée. Comme cet aquarium équipé d'un système IoT était segmenté de manière inappropriée sur le réseau du casino, les pirates ont pu se déplacer latéralement dans l'infrastructure en Cloud du casino et poursuivre leur attaque. (Wei)

Appareils médicaux

L'attaque du ransomware WannaCry en 2017 a incité les fabricants et les agences gouvernementales à reconsidérer les vulnérabilités des dispositifs médicaux connectés à Internet, notamment les pompes à insuline et les stimulateurs cardiaques. (Chase, Coley et Connolly)

Véhicules

2015 : des pirates informatiques ont détourné une Jeep Cherokee, coupant son moteur en plein trajet sur l'autoroute. (Greenburg)

2023 : un conducteur de Tesla a découvert que l'application mobile officielle de Tesla lui permettait d'entrer, et de conduire un véhicule qu'il ne possédait pas. (Day)

Après 2023 : les représentants du gouvernement avertissent qu'« il n'existe actuellement aucune approche globale [...] en matière de cybersécurité » pour les véhicules électriques ou leurs chargeurs (SANDIA) ; véhicules que les employés des organisations conduiront pour se rendre au bureau ou à des réunions hors site, et auxquels ils connecteront leurs appareils professionnels par Bluetooth.

Répercussions dans le monde réel

Le quasi-piratage d'Equifax par l'homme du milieu

L'une des attaques les plus courantes contre les appareils mobiles et les terminaux est celle de l'homme du milieu (MitM). Lorsque des employés se connectent à des informations sensibles sur un réseau ou une connexion Internet non sécurisés, les pirates peuvent se placer au milieu du flux de données et « attraper » toute information exclusive.

La perspective d'une attaque MitM est la raison pour laquelle Equifax, une société américaine d'information sur le crédit à la consommation, a retiré ses applications d'Apple et de Google en 2017.

Suite à l'exposition scandaleuse de quelque 143 millions de données personnelles de clients à des pirates infiltrés dans leur réseau pendant des mois en raison de l'absence de correction d'une vulnérabilité exploitée connue (Khandelwal), le chercheur en sécurité Jerry Decime s'est interrogé : après cette violation, Equifax avait-elle renforcé sa sécurité dans l'ensemble de l'organisation ?

Decime a examiné les versions des applications mobiles du logiciel d'Equifax et, à sa grande surprise, a découvert que les applications ne maintenaient pas l'utilisation des protocoles HTTPS après l'authentification initiale dans une série de domaines critiques. (Decime)

Toute information transmise après l'authentification entre l'appareil de l'utilisateur et les serveurs d'Equifax, notamment des informations plus personnelles et des transactions financières aurait pu être interceptée et exfiltrée par un pirate intelligent réalisant que leur sécurité n'était que superficielle.

Equifax a eu le mérite de répondre à la communication de Decime dans l'heure qui a suivi et de retirer les applications non sécurisées des places de marché d'Apple et de Google. (Weissman)

Cependant, cet exemple classique d'une (presque) attaque MitM souligne l'importance vitale d'une communication sécurisée entre un utilisateur et le serveur d'une entreprise, ou bien entre vos employés et les informations et réseaux sensibles de votre organisation.

Les solutions UEM et les outils de sécurité des partenaires peuvent limiter de manière proactive l'exposition à ces types d'attaques :

- des profils d'accès utilisateur robustes ;
- le dé-provisionnement automatique des informations d'identification ;
- l'accès sécurisé aux données et canaux de communication, tels que les VPN ou les contrôles « zéro confiance », également déployés et surveillés via les solutions UEM.

3

L’application de politiques de sécurité et l’enregistrement des appareils empêchent les pirates de prendre pied dans les réseaux de l’entreprise.

Les stratégies de cybersécurité proactives visent non seulement à empêcher les pirates de s’introduire dans les réseaux de l’entreprise, mais aussi à prévoir les conséquences de cette intrusion.

Prenez l’exemple de l’humble clé USB. Elle peut contenir des fichiers volumineux tels que des présentations, des vidéos et de la musique à utiliser sur de nouveaux ordinateurs sans nécessiter de connexion réseau pour charger ou télécharger du matériel.

Bien entendu, si les clés USB peuvent transporter des fichiers volumineux à des fins légitimes, elles peuvent également transporter des logiciels malveillants.

Les solutions UEM peuvent déployer et appliquer automatiquement par défaut des politiques relatives aux supports amovibles. Grâce à ces politiques, les utilisateurs finaux de votre entreprise doivent demander une autorisation spéciale pour utiliser des dispositifs porteurs de mémoire avec les appareils appartenant à l’entreprise, plutôt que de laisser chaque appareil et chaque terminal automatiquement exposés à ces attaques.

Répercussions dans le monde réel

Stuxnet : le logiciel malveillant sur clé USB le plus célèbre au monde

Stuxnet est le nom donné à un virus informatique qui aurait été conçu par certaines agences de renseignement pour faire échouer le programme d'enrichissement nucléaire de l'Iran.

L'installation fonctionnait sous la plus haute sécurité, c'est-à-dire qu'elle était isolée de tout accès à Internet ou réseau extérieur. Le seul moyen pour un logiciel malveillant de pénétrer à l'intérieur de l'installation était qu'une personne de confiance l'introduise personnellement dans un ordinateur du réseau de l'installation.

Les attaquants ont donc créé un virus informatique qui s'attaquait uniquement aux systèmes de contrôle industriel utilisés par l'installation iranienne pour les centrifugeuses et ont chargé l'ensemble des logiciels malveillants sur des clés USB.

Les clés contaminées ont été distribuées dans toute la région pour que les scientifiques nucléaires les trouvent, peut-être lors de conférences, ou tout simplement distribuées par des collègues de confiance dans la région.

Enfin, un scientifique a commis l'erreur fatale de brancher une clé USB contenant le logiciel malveillant Stuxnet… et le programme a perdu environ 1 000 centrifugeuses et gaspillé du matériel, obligeant ainsi les dirigeants iraniens à signer l'accord sur le nucléaire iranien de 2015.

Pour en savoir plus sur Stuxnet, consultez les ressources suivantes :

- « Ep 29 : Stuxnet » par Jack Rhysider
- « Compte à rebours vers le jour zéro : Stuxnet et le lancement de la première arme numérique au monde » par Kim Zetter

Les journaux des appareils et des utilisateurs enregistrés par une plateforme UEM peuvent également être utilisés à des fins de sécurité.

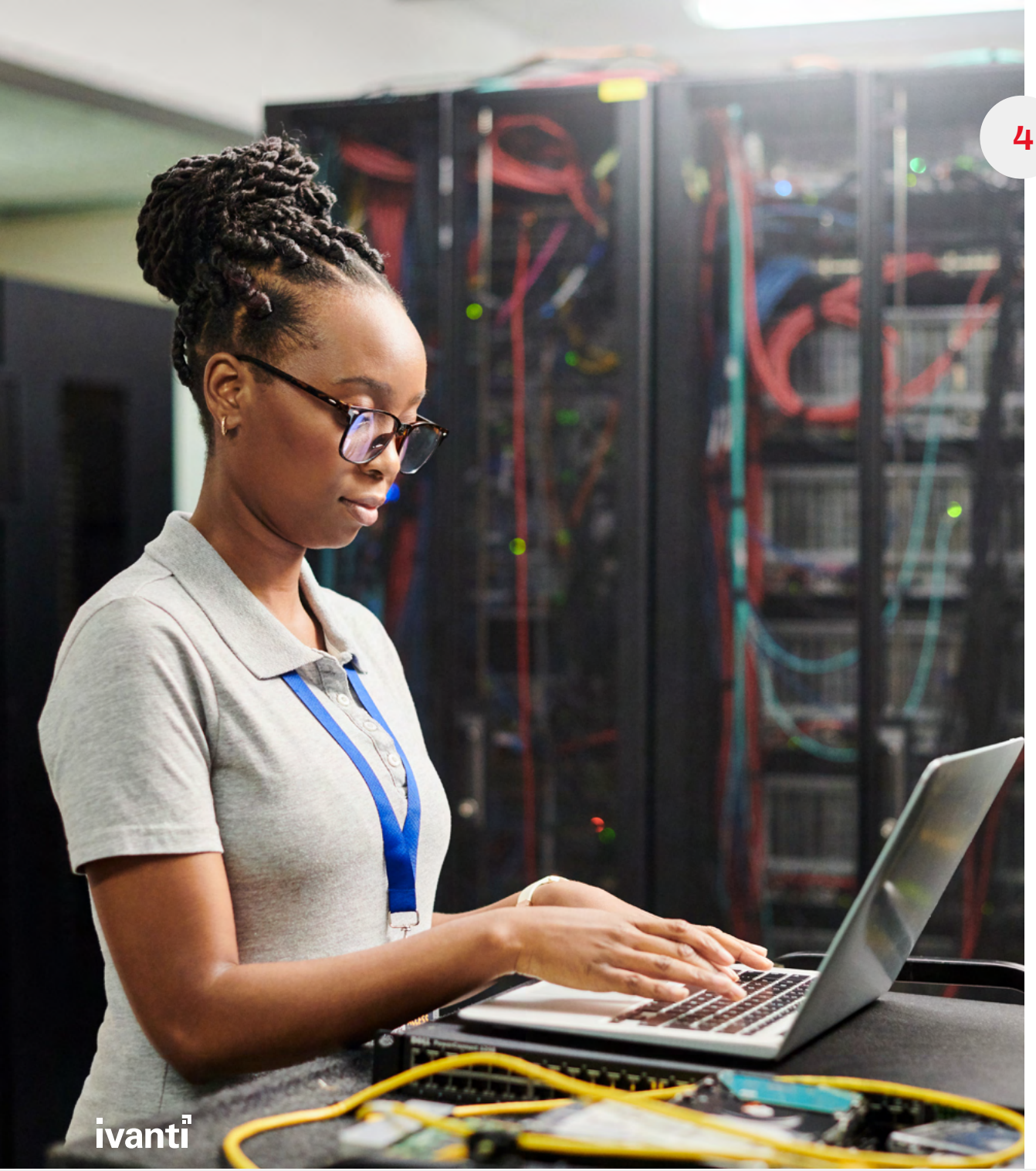
Si l'organisation a des raisons de penser qu'un employé présente une menace interne, les équipes de sécurité peuvent vérifier les enregistrements d'un appareil à la recherche de signes indiquant que des outils de niveau administrateur système, tels que PowerShell, ont été illégalement installés et utilisés sur l'appareil d'un utilisateur.

Ou encore, le système d'une organisation alerte sur l'activité d'un « utilisateur » ordinaire, révélant que ce dernier a soudainement mis en œuvre des techniques de réseau avancées sur l'appareil géré par l'organisation.

De telles activités peuvent être le signe qu'il ne s'agit absolument pas de l'utilisateur autorisé, mais plutôt d'un pirate qui se cache derrière ses identifiants authentiques (mais compromis) et essaie d'escalader ses privilèges au sein du réseau de l'entreprise.

Avec les configurations, les alertes et les outils de sécurité appropriés, ces activités pourraient être détectées sur un terminal ou un appareil mobile bien avant que le pirate ne se déplace latéralement dans le réseau de l'entreprise ou n'obtienne des autorisations de niveau administrateur.

Et à mesure que l'augmentation des taux de cyber-assurance accroît la pression sur les finances déjà tendues des organisations, les équipes informatiques et de sécurité peuvent juger très économique d'appliquer des politiques plus strictes en matière de supports amovibles et d'alertes sur l'activité des utilisateurs pour une remédiation proactive des risques et une réduction des primes d'assurance. (Breg)



4

Les intégrations faciles offrent des implémentations de sécurité simples, uniques.

Bien qu'une plateforme UEM correctement intégrée offre des possibilités d'hygiène cybernétique de base, elle ne peut pas être la panacée de vos solutions de sécurité des terminaux.

Cependant, les solutions UEM offrent une rampe de lancement extrêmement bien positionnée pour d'autres outils, tels que la gestion des correctifs ou les solutions de défense contre les menaces mobiles. Après tout, l'UEM lui-même dispose d'un client directement installé sur chaque appareil appartenant et géré par l'organisation.

Il suffit de quelques clics pour que d'autres outils de sécurité soient connectés à ce même appareil via le client UEM, renforçant immédiatement vos défenses de sécurité des terminaux sans nuire à la DEX de votre organisation ou à la productivité de l'utilisateur final.

UEM + Gestion des correctifs basée sur les risques

Par exemple, les UEM peuvent être associés à des solutions de gestion des correctifs et des vulnérabilités basées sur les risques pour une réponse proactive transparente aux risques, afin de remédier aux vulnérabilités activement exploitées dans votre environnement actuel.

1 **L'équipe de sécurité analyse les données de renseignement sur les menaces actuelles,** en recherchant les vulnérabilités récemment exploitées dans les appareils et les applications actuellement utilisés par votre organisation.

- Les capacités d'analyse active de l'UEM assurent de ne laisser échapper aucun appareil ou application au cours de cette évaluation initiale !

2 **L'équipe de sécurité priorise ou accélère les vulnérabilités actuelles non corrigées,** en fonction de l'environnement de risque et des priorités de votre organisation. Elle peut envisager :

- le niveau de priorité des appareils, utilisateurs, systèmes d'exploitation et fonctions critiques de l'entreprise potentiellement touchés ;
- si une vulnérabilité a été activement exploitée par des acteurs dangereux connus du grand public ;
- le type d'accès ou d'autorisations qu'une exploitation pourrait accorder à un acteur de la menace ;
- la fréquence d'utilisation par l'organisation, de manière passive ou active, des appareils ou des applications potentiellement touchés ;
- La difficulté d'application d'un correctif ou la nécessité de procéder à d'autres mesures correctives (mise en quarantaine, segmentation, etc.).

3 **L'équipe informatique reçoit une liste de correctifs classés par ordre de priorité,** ainsi que :

- des informations sur les raisons pour lesquelles ces correctifs devraient être appliqués, sur la base des facteurs de risque propres à l'organisation, permettant de rassurer l'équipe informatique sur le fait que la sécurité ne lui demande pas de corriger toutes les vulnérabilités possibles !
- des dispositifs ou des utilisateurs spécifiques pour le déploiement des correctifs, selon des cadences prédéterminées.
- les interférences possibles connues avec les suites logicielles ou les flux de travail actuels.

4 **L'équipe informatique déploie automatiquement les correctifs sur les appareils et les terminaux identifiés via la plateforme UEM,** planifiant les mises à jour pour minimiser l'impact sur la productivité de l'utilisateur final et en gardant un œil sur toute activité étrange indiquant l'interférence d'un correctif avec les flux de travail habituels.

Pour en savoir plus sur les stratégies de correctifs et de remédiation basées sur le risque, veuillez consulter le Guide ultime de la gestion des correctifs basée sur le risque.

UEM + défense contre les menaces mobiles

Tout le monde est vulnérable à l'hameçonnage, même les professionnels !

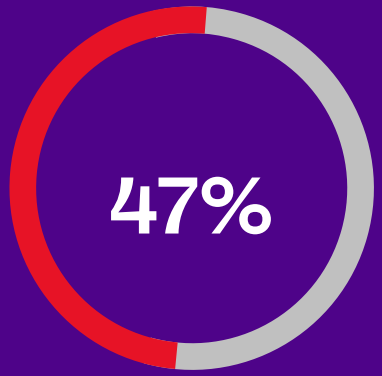
Les campagnes d'hameçonnage sont un point d'entrée connu pour les gangs de ransomware en particulier, représentant 54 % de toutes les méthodes de transmission de ransomware en 2020. (Datto)

Les attaques d'hameçonnage spécialisées de type « whaling » - des campagnes d'e-mails conçues par des pirates et ciblant spécifiquement les dirigeants de grandes entreprises - ont entraîné pour les sociétés américaines des pertes estimées à 2,4 milliards de dollars en 2021. (Verizon)

De nouvelles recherches ont révélé :

- 47 % des professionnels de l'informatique admettent être tombés dans le piège d'une attaque par hameçonnage. (Ivanti)
- Seuls 43 % des professionnels de la sécurité affirment que leur entreprise a subi une attaque par hameçonnage au cours des 24 derniers mois (Ivanti), alors que d'autres rapports sectoriels indiquent que 83 % des entreprises ont subi une attaque par hameçonnage réussie en 2021 (Verizon).
- Plus d'un tiers des cadres supérieurs admettent avoir cliqué sur un lien d'hameçonnage, soit quatre fois plus que les autres employés de bureau. (Ivanti)

Il y a un écart de 40 points entre le nombre d'attaques par hameçonnage estimé par les équipes de sécurité et le nombre d'attaques par hameçonnage réellement perpétrées.



des professionnels de l'informatique ont été victimes d'attaques par hameçonnage.

Donc, si :

- Des informaticiens sont victimes d'e-mails d'hameçonnage
- Les spécialistes de la sécurité ne se rendent pas compte que leur organisation est victime d'attaques par hameçonnage
- Les cadres supérieurs sont de plus en plus souvent ciblés, et de plus en plus souvent victimes de ces attaques

... la formation en matière de sécurité et les filtres anti-spam dans les boîtes de réception des organisations ne suffisent donc pas à arrêter les utilisateurs qui compromettent la sécurité des organisations par des campagnes d'hameçonnage.

Si les configurations et les paramètres d'un UEM peuvent contribuer à limiter les dommages initiaux causés par un clic sur un lien d'hameçonnage - en particulier s'il a été associé à une solution de correctifs, limitant de manière significative la capacité des pirates à escalader leurs privilèges ou à se déplacer dans le réseau - il ne sera pas aussi efficace s'il n'est pas associé à une solution spécialisée de défense contre les menaces mobiles (MTD).

Les solutions MTD les plus performantes peuvent s'exécuter via le client UEM d'un appareil enregistré - qu'il soit détenu par l'entreprise ou intégré à un programme BYOD - sans interférer avec les activités régulières de l'utilisateur ni consommer de mémoire supplémentaire.

Si la solution MTD détecte :

- **un lien d'hameçonnage entrant :** le système bloque immédiatement le mouvement et veille à ce que l'utilisateur ne termine pas l'action.
- **une activité potentiellement malveillante :** les solutions MTD et UEM procèdent alors automatiquement à différents niveaux de remédiation, en fonction de l'activité spécifique et du niveau de menace potentielle - jusqu'à supprimer l'accès de l'utilisateur à toutes les applications de l'entreprise, et ce, même sur l'appareil appartenant à l'utilisateur ! - jusqu'à ce que l'utilisateur ait supprimé l'application ou résolu le problème.
- **Une mise à jour du système d'exploitation non installée :** le système propose poliment une notification push à l'utilisateur, l'encourageant à installer la mise à jour. Si l'utilisateur refuse systématiquement de mettre à jour son appareil, des mesures correctives de plus en plus importantes sont mises en œuvre, pouvant aller jusqu'à la mise en quarantaine des applications de l'organisation ou de l'accès à partir de l'appareil non mis à jour.

04

Comment choisir votre solution UEM

Il existe de nombreuses solutions UEM performantes. Si la plupart d'entre elles offrent les fonctionnalités de base décrites dans ce guide, chaque fournisseur propose des fonctionnalités uniques.

Comment choisir le fournisseur de solutions UEM qui convient à votre organisation ? Un fournisseur en mesure de répondre à vos besoins actuels, mais aussi d'évoluer et offrir de nouvelles possibilités pour des contrôles et une sécurité toujours plus performants à mesure que les besoins de votre organisation évoluent ?

Votre solution de gestion unifiée des terminaux doit :

- ☐ **prendre en charge toute la gamme d'appareils et de systèmes d'exploitation** que votre organisation utilise actuellement - ou pourrait utiliser à l'avenir - y compris macOS, iOS, iPadOS, Windows, ChromeOS, Android et Linux ;
- ☐ **offrir un tableau de bord à « écran unique »** contenant des informations sur les périphériques et l'activité des utilisateurs afin que les équipes informatiques et de sécurité puissent travailler à partir du même jeu de données ;
- ☐ **prendre en charge les déploiements sur site et dans le Cloud**, y compris les applications natives du Cloud, et ce même si une organisation pense qu'elles sont « uniquement » au bureau !
- ☐ **agréger et rendre compte clairement des informations sur les utilisateurs et les appareils** afin d'informer les stratégies plus larges sur les actifs informatiques et les terminaux de sécurité, comme les accords de licence logicielle ou les stratégies de correctifs basées sur les risques ;
- ☐ **faciliter les enrôlements et déploiements simples et automatiques des périphériques ;**
- ☐ **fonctionner de manière aussi discrète et « invisible » que possible**, offrant ainsi aux utilisateurs finaux une expérience technologique positive tout en corrigeant les problèmes de manière proactive et en permettant un « shift left » aux équipes informatiques afin de se consacrer à des initiatives plus stratégiques que la résolution de simples tickets de service d'assistance ;
- ☐ **s'intégrer de manière native aux outils de sécurité des terminaux connexes**, tels que les solutions de gestion des correctifs et des vulnérabilités basées sur les risques et les produits de défense contre les menaces mobiles, car une plateforme UEM ne peut pas tout faire toute seule - et fuyez tout fournisseur qui tente de vous dire le contraire !
- ☐ **mettre en œuvre des automatisations standard, des accords de niveau de service et des alertes** telles que des protocoles de dé-provisionnement, des procédures d'intégration, des pics d'activité ou des décalages, des comportements de jailbreaking d'applications malveillantes, des déploiements de correctifs approuvés, etc.

Répercussions dans le monde réel

L'étude Total Economic Impact™ pour Ivanti Neurons for UEM

Une étude de juillet 2022 portant sur l'impact économique total (Total Economic Impact™), réalisée par Forrester Consulting à la demande d'Ivanti, a révélé qu'en mettant en œuvre Ivanti Neurons for UEM, une entreprise de taille moyenne gérant 10 000 terminaux et connaissant une croissance annuelle de 5 % a enregistré des bénéfices de 2,24 millions de dollars sur trois ans, contre des coûts de 619 000 dollars. (Étude TEI de Forrester Consulting)

Ces avantages se sont traduits par une valeur actuelle nette (VAN) de 1,62 million de dollars et un retour sur investissement de 261 % sur trois ans, avec une période de récupération de l'investissement initial de l'organisation composite dans les six mois suivant l'installation. (Étude TEI de Forrester Consulting)

Selon la même étude commandée par le TEI, ces économies ont été réalisées grâce aux éléments suivants :

- consolidation de la pile technologique
- licences logicielles récupérées
- automatisation des correctifs
- amélioration de la productivité des utilisateurs
- intégration et provisionnement en libre-service

Avantages (sur trois ans) pour l'ensemble de l'organisation

Selon les personnes interrogées dans le cadre de l'étude commandée par le TEI

Intégration en libre-service et approvisionnement automatisé
$716 632 d'économies sur 3 ans pour une organisation composite

« Nous avons développé avec Ivanti un formulaire d'onboarding qu'un superviseur peut soumettre à l'aide du portail en libre-service. Il crée automatiquement un ticket et le transmet aux équipes concernées. Nous n'avons pas besoin de remplir une checklist comme effectué auparavant. »

(La personne interrogée a en outre estimé que le temps consacré par les informaticiens au processus d'onboarding était réduit de 50 %)

- Spécialiste informatique d'une agence gouvernementale

Consolidation de la pile technologique et mise à l'écart des outils existants
$358 734 d'économies sur 3 ans pour une organisation composite

« Ma solution de contrôle à distance coûtait $75 000 par an. Ma solution de [gestion des actifs informatiques] (ITAM) représentait $100 000 de plus. La gestion des connaissances représentait $20 000 de plus par an... Si je fusionne avec un seul fournisseur et que je regroupe tous ces coûts, je peux économiser. »

- Directeur de l'informatique et de l'assistance télécom pour une entreprise de soins palliatifs

Capacités d'automatisation des correctifs et intégrations
$162 515 d'économies sur 3 ans pour une organisation composite

« Il nous a fallu un mois pour concevoir et discuter de la manière d'automatiser les correctifs. Une fois la politique élaborée, il nous a fallu moins d'une heure pour mettre en place un projet de déploiement, puis les correctifs ont tout simplement été appliqués. Je n'ai pas à m'en charger et j'ai la certitude que ce que je vois est exact. »

- Responsable de l'intégration pour un détaillant de chaussures

Licences de logiciels récupérées
$439 449 d'économies sur 3 ans pour une organisation composite

« Auparavant, si nous voulions récupérer des logiciels, le processus était très long puisque nous devions contacter les utilisateurs pour leur demander : « Vous n'avez pas utilisé ce logiciel depuis un certain temps, pouvons-nous le retirer ? » En intégrant nos licences logicielles à la solution EPM [qui fait partie d'Ivanti Neurons for UEM], nous sommes désormais en mesure de récupérer automatiquement les logiciels [...] C'est probablement la plus grande économie que nous ayons réalisée dans ce domaine. »

- Responsable de l'infrastructure et des services de livraison de terminaux pour une entreprise de production alimentaire

Amélioration de la productivité des utilisateurs finaux
$560 521 d'économies sur 3 ans pour une organisation composite

« En effectuant une partie de l'autoréparation - mise à jour des anciens profils, redémarrage des ordinateurs s'ils n'ont pas été redémarrés depuis sept jours, application de correctifs le soir - ce travail a aidé nos utilisateurs finaux à devenir plus productifs puisque les ordinateurs récupèrent une partie des ressources qui étaient accaparées auparavant [...] Chaque minute gagnée représente un avantage financier pour l'utilisateur final. »

- Directeur de l'informatique et de l'assistance télécom pour une entreprise de soins palliatifs

Pour plus d'informations, veuillez lire l'impact économique total™ des solutions de gestion unifiée des terminaux (UEM) d'Ivanti.

Références

1. Bitwarden. 2022 Password Decisions Survey. November 2021. https://bitwarden.com/images/resources/2022-password-decisions-survey.pdf.
2. Bond, Shannon. Twitter employees quit in droves after Elon Musk's ultimatum passes. 17 November 2022. https://www.npr.org/2022/11/17/1137413251/twitter-employees-quit-elon-musk.
3. Bonner, Carole. Health and Wellbeing for the Remote & Hybrid Workforce. 20 October 2022. https://8926463.fs1.hubspotusercontent-na1.net/hubfs/8926463/Remote%20Hybrid%20Workforce_Formatted.pdf.
4. Brasen, Steve. Evolving Requirements for Digital Employee Experience (DEX). 4 August 2022. https://www.ivanti.com/resources/v/doc/ebooks/ema-iva009a-ivanti-requirements-ebook.
5. Breg, David. Quarterly Cyber Insurance Update. 10 February 2023. https://www.wsj.com/articles/quarterly-cyber-insurance-update-february-2023-62141c19.
6. Chase, Melissa, et al. Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook. 14 November 2022. https://www.mitre.org/news-insights/publication/medical-device-cybersecurity-regional-incident-preparedness-and-response.
7. Cipolla, Tom, et al. Magic Quadrant for Unified Endpoint Management Tools. 1 August 2022. https://www.gartner.com/doc/reprints?id=1-2AQEK9FU&ct=220802&st=sb.
8. Datto. Datto's Global State of the Channel Ransomware Report. November 2020. https://www.datto.com/resource-downloads/Datto-State-of-the-Channel-Ransomware-Report-v2-1.pdf.
9. Day, Lewin. Tesla App Unlocks Someone Else's Car, Lets Them Drive Away in It. 14 March 2023. https://www.thedrive.com/news/tesla-app-unlocks-someone-elses-car-lets-them-drive-away-in-it.
10. Decime, Jerry. Settling the score: taking down the Equifax mobile application. n.d. https://www.linkedin.com/pulse/settling-score-taking-down-equifax-mobile-application-jerry-decime/.
11. Flexera Software. 2021 State of IT Visibility Report. June 2021. https://info.flexera.com/ITV-REPORT-State-of-IT-Visibility.
12. Forrester Consulting study commissioned by Ivanti. The Total Economic Impact™ Of Ivanti Unified Endpoint Management (UEM) Solutions. July 2022. https://rs.ivanti.com/reports/forrester-tei-of-ivanti-uem-solutions-2022.pdf.
13. Greenburg, Andy. Hackers Remotely Kill a Jeep on the Highway—With Me in It. 21 July 2015. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
14. IBM Security. X-Force Threat Intelligence Index 2022. February 2022. https://www.ibm.com/downloads/cas/ADLMYLAZ.
15. Insight Enterprises & CIO. Insight intelligent technology report 2022: IT ambions for business transformation. November 2021. https://ca.insight.com/en_CA/content-and-resources/gated-content/insight-intelligent-technology-report-ac1252.html.
16. Ivanti. 2022 Digital Employee Experience Report. 28 June 2022. https://rs.ivanti.com/ivi/2700/4e528f833de3.pdf.
17. —. 9 Must-Know Phishing Attack Trends. 20 July 2021. https://www.ivanti.com/resources/v/doc/ivi/2732/7b4205775465.
18. —. Getting Started With DEX: Core Areas of Focus to Deliver a Great Digital Employee Experience. 23 Novemer 2022. https://rs.ivanti.com/ivi/2734/f6efbc801083.pdf.
19. —. Government Cybersecurity Status Report. 9 March 2023. https://www.ivanti.com/resources/v/doc/ivi/2747/a856c631661d.
20. —. Press Reset: A 2023 Cybersecurity Status Report. December 2022. https://www.ivanti.com/lp/security/assets/s1/2023-cybersecurity-status-report.
21. Khandelwal, Swati. Equifax Suffered Data Breach After It Failed to Patch Old Apache Struts Flaw. 14 September 2017. https://thehackernews.com/2017/09/equifax-apache-struts.html.
22. Kolodny, Lora. Twitter is down to fewer than 550 full-time engineers. 20 January 2023. https://www.cnbc.com/2023/01/20/twitter-is-down-to-fewer-than-550-full-time-engineers.html.
23. Lutkevich, Ben. Wi-Fi Pineapple. October 2022. https://www.techtarget.com/searchsecurity/definition/Wi-Fi-Pineapple.

Références

24. Morning Consult and IBM. IBM Security Incident Responder Study. 3 October 2022. https://www.ibm.com/downloads/cas/XKOY5OLO.

25. NASCIO. The 2021 State CIO Survey. October 2021. https://www.nascio.org/wp-content/uploads/2021/10/2021-State-CIO-Survey.pdf.

26. Palmer, Annie. Amazon employees push CEO Andy Jassy to drop return-to-office mandate. 21 February 2023. https://www.cnbc.com/2023/02/21/amazon-employees-push-ceo-andy-jassy-to-drop-return-to-office-mandate.html.

27. Paychex. Feeling the Burn(out): Exploring How Employees Overcome Burnout. 25 February 2019. https://www.paychex.com/articles/human-resources/impact-of-employee-burnout.

28. Proofpoint. 2022 Voice of the CISO: Global Insights Into CISO Challenges, Expectations and Priorities. May 2022. https://www.proofpoint.com/sites/default/files/white-papers/pfpt-us-wp-voice-of-the-CISO-report.pdf.

29. PwC. 2022 Global Digital Trust Insights. December 2021. https://www.pwc.se/sv/pdf-reports/cybersecurity/cyber-global-digital-trust-insights-2022.pdf.

30. Rhysider, Jack. Darknet Diaries, Episode 68: Triton. June 2020. https://darknetdiaries.com/transcript/68/.

31. Rundle, James. “Economic Uncertainty Weighs on Cyber Chiefs.” Wall Street Journal 13 January 2023. https://www.wsj.com/articles/economic-uncertainty-weighs-on-cyber-chiefs-11673562985.

32. SAM. IoT Security Landscape Report. July 2022. https://securingsam.com/wp-content/uploads/2022/04/SAM_IOT-Security-Report.pdf.

33. SANDIA. Cybersecurity for Electric Vehicles Charging Infrastructure. July 2022. https://www.osti.gov/servlets/purl/1877784/.

34. Shackleford, Dave. SANS 2022 Cloud Security Survey. March 2022. https://8645105.fs1.hubspotusercontent-na1.net/hubfs/8645105/white-paper/sans-2022-cloud-security-survey.pdf.

35. Shumway, Emilie. Monster: Two-thirds of workers would quit if forced to return to the office five days a week. 26 September 2022. https://www.hrdive.com/news/monster-two-thirds-workers-would-quit-forced-back-to-office/632690/.

36. Smith, Ray A. Quiet Quitters Make Up Half the U.S. Workforce, Gallup Says. 29 September 2022. https://www.wsj.com/articles/quiet-quitters-make-up-half-the-u-s-workforce-gallup-says-11662517806.

37. Tsipursky, Gleb. The return to the office could be the real reason for the slump in productivity. Here’s the data to prove it. 16 February 2023. https://fortune.com/2023/02/16/return-office-real-reason-slump-productivity-data-careers-gleb-tsipursky/.

38. Vanson Bourne for Nutanix. Nutanix Enterprise Cloud Index: Application Requirements to Drive Hybrid Cloud Growth (2019 edition). November 2019. https://www.nutanix.com/content/dam/nutanix/resources/gated/analyst-reports/enterprise-cloud-index-2019.pdf.

39. Verizon. Mobile Security Index 2022. 2022 August 2. https://www.verizon.com/business/resources/reports/2022-msi-report.pdf.

40. Wei, Wang. Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer. 16 April 2018. https://thehackernews.com/2018/04/iot-hacking-thermometer.html.

41. Weissman, Cale Guthrie. Here’s Why Equifax Yanked Its Apps From Apple And Google Last Week. 15 September 2017. https://www.fastcompany.com/40468811/heres-why-equifax-yanked-its-apps-from-apple-and-google-last-week.

42. Wilson, Dan, et al. Market Guide for DEX Tools. 31 August 2022. https://www.gartner.com/doc/reprints?id=1-2B07Z49S&ct=220902&st=sb.

43. Yang, Mary. Elon Musk gives Twitter employees an ultimatum: Stay or go by tomorrow. 16 November 2022. https://www.npr.org/2022/11/16/1137105935/twitter-elon-musk-ultimatum.

Le guide ultime de la gestion unifiée des terminaux

Comment les solutions modernes de gestion des terminaux impactent la sécurité et l'expérience des employés

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

Copyright © 2023, Ivanti. Tous droits réservés. IVI-2747 NH/MM