ivanti

Tracez votre parcours de cybersécurité (M.A.P.)

Six étapes pour définir une approche de cybersécurité pour l'Everywhere Workplace

Table des matières

Pourquoi cet eBook ?	2
Introduction	3
Votre parcours de cybersécurité (M.A.P)	4
Étape 1 : Bénéficiez d'une visibilité complète sur l'ensemble des biens	5
Étape 2 : Modernisez la gestion des périphériques	6
Étape 3 : Mettez en place une bonne hygiène des périphériques	7
Étape 4 : Sécurisez vos utilisateurs	9
Étape 5 : Fournissez un accès sécurisé	10
Étape 6 : Gérez la conformité et les risques	11
Tracez votre parcours de cybersécurité (M.A.P.)	12
À propos d'Ivanti	13

Pourquoi cet eBook?

Vulnérabilités de logiciels, malwares, vols d'identifiants, et autres vecteurs de menace pèsent sur le quotidien des entreprises. Ces menaces connaissent une croissance exponentielle, à la fois dans leur fréquence et leur sophistication. Le développement de l'Everywhere Workplace et la généralisation subite du télétravail, ainsi que les restrictions budgétaires et la pénurie de compétences en sécurité n'ont fait qu'aggraver ce problème. La gestion des alertes de vulnérabilités était déjà difficile, mais c'est aujourd'hui quasiment impossible.

Pour les entreprises (et donc pour le département IT), la situation exige la mise en place d'une stratégie visant à renforcer la sécurité, gérer en continu des risques de cybersécurité et limiter les perturbations. Pour ce faire, il faut regarder plus loin que les solutions conçues pour un environnement composé de PC et de centres de données. C'est le moment d'adopter des solutions conçues pour l'Everywhere Workplace, ce nouvel environnement de travail centré sur les technologies mobiles et Cloud.

Ce guide vous servira de point de départ et de feuille de route tout au long de votre parcours de cybersécurité. Vous souhaitez améliorer la protection des utilisateurs, des périphériques, des réseaux, des applications et des données contre la multiplication des menaces dans l'Everywhere Workspace ? Suivez nos recommandations !

Le paysage actuel de la cybersécurité

Il ne s'agit plus seulement de menaces, mais bien réellement d'attaques. Comment en est-on arrivé là ?

L'essor rapide de l'Everywhere Workplace a provoqué une multiplication spectaculaire des points d'exposition vulnérables. Initialement considéré comme temporaire, cet environnement de travail digital à distance va perdurer : l'Everywhere Workplace est là pour de bon. D'après Gartner[1], 82 % des entreprises prévoient d'autoriser le télétravail à temps partiel et 47 % souhaitent à l'avenir laisser leur personnel télétravailler à temps complet. Il est devenu évident que les solutions de sécurité centrées sur les PC et les bases de données, en vogue avant la pandémie, ne sont plus adaptées à la situation actuelle (des collaborateurs répartis géographiquement qui utilisent principalement des périphériques mobiles et des applications Cloud).

Les QR codes que nous utilisons quotidiennement en sont un bon exemple. Ils se sont répandus partout, des restaurants aux cabinets médicaux, et ils sont souvent scannés avec les périphériques mobiles que les collaborateurs utilisent à des fins professionnelles. Mais l'ubiquité et la facilité d'emploi des QR codes en font également un vecteur idéal pour les attaques par hameçonnage. Si les seules solutions en place sont des solutions antihameçonnage pour e-mail, l'utilisateur et l'entreprise s'exposent à des attaques.

Pire encore, les menaces de tous types sont devenues plus sophistiquées. Elles ciblent souvent spécifiquement les vulnérabilités générées par le télétravail, et leur fréquence est alarmante. Les tentatives d'hameçonnage, par exemple, ont augmenté de 85 % par rapport à l'année précédente (74 % des entreprises en ont été victimes), et 59 % des entreprises ont signalé avoir été victimes d'un ransomware (ou rançongiciel) en 2021. Si l'on y ajoute la pénurie mondiale d'experts en cybersécurité et les restrictions budgétaires, on constate que les équipes IT et Sécurité dédient jusqu'à 53 %[2] de leur temps à des tâches liées à l'organisation et à la priorisation des vulnérabilités.

C'est un tsunami : nous vivons une transformation du lieu de travail, il y a trop d'éléments à sécuriser et pas assez de ressources pour agir. Il faut garder le cap, on n'a plus le choix. Les entreprises qui n'y parviennent pas vont probablement subir plus de failles de sécurité, notamment les ransomwares, l'hameçonnage, les piratages et les vulnérabilités causées (volontairement ou non) par les collaborateurs en interne, et potentiellement enfreindre des obligations de conformité. L'impact sur la marque est incalculable : interruptions imprévues, problèmes de conformité, perte de réputation et de clients, et un coût estimé à 4,24 millions de dollars par fuite de données[3]. Les attaques par rançongiciel provoquent une interruption qui dure en moyenne 22 jours[4]. Les violations de conformité ont, quant à elles, coûté aux entreprises plus de 1,3 milliard de dollars… et ce n'est pas fini.[5]

"C'est un tsunami : nous vivons une transformation du lieu de travail, il y trop d'éléments à sécuriser et pas assez de ressources pour agir."

Votre parcours de cybersécurité (M.A.P)

L'acronyme M.A.P. correspond à l'anglais Manage, Automate, and Prioritize (Gérer, automatiser, prioriser) et désigne un parcours en trois phases permettant de créer une stratégie de cybersécurité complète, évolutive et alignée sur les besoins de l'Everywhere Workplace.

Gérer, la première phase, consiste à poser les bases de votre cybersécurité. Son objectif : vous permettre de passer d'un état inconnu à un état connu. Cela signifie gagner en visibilité sur l'identité des utilisateurs, sur les périphériques et sur les applications qu'ils utilisent afin de mieux comprendre où se trouvent vos vulnérabilités. Cela signifie également oublier les pratiques susceptibles de mettre votre entreprise en danger, comme autoriser des périphériques non gérés à accéder aux ressources d'entreprise (et tout particulièrement à celles situées dans le Cloud) ou retarder l'application des correctifs récents.

Automatiser, la deuxième étape, vise à alléger la charge de travail. Une fois que vous avez atteint un état connu, l'étape suivante consiste à libérer des ressources en automatisant les processus manuels répétitifs, comme la maintenance de l'inventaire, l'intégration de nouveaux périphériques, et le déploiement des espaces de travail et des applications. Vous pouvez également y ajouter des solutions d'autoréparation et de self-service pour réduire encore plus les interventions du département IT.

Enfin, pour la phase **Prioriser**, l'objectif est que le département IT possède les informations et les outils qui lui permettent d'identifier et de traiter les risques les plus élevés. Malgré l'automatisation, certains aspects vont toujours nécessiter l'intervention des équipes IT.

En s'affranchissant d'une approche de gestion des risques faite d'approximations et d'estimations, le département IT est à même de prendre des décisions intelligentes et stratégiques basées sur des données fiables et des scores de risque.

Même s'il est propre à chaque entreprise, un programme M.A.P. doit toujours reposer sur les cinq piliers essentiels que sont les utilisateurs, les périphériques, le réseau, les applications et les données, et inclure des facteurs comme :

- La découverte des biens
- La gestion des biens
- L'application et la vérification d'une configuration sécurisée
- Les systèmes d'application des correctifs basés sur les risques, correctement mis à jour
- La réduction des risques créés par les collaborateurs via des méthodes comme les authentifications vérifiées
- Un contrôle adaptatif et la gestion du cycle de vie

Même si elle n'empêche pas toutes les attaques, cette approche réduit la surface d'attaque tout en permettant une gestion intelligente et proactive des risques. Vous êtes ainsi mieux préparé. Avec une gestion en continu des risques de cybersécurité, votre entreprise est mieux protégée : réduction de l'exposition aux risques et limitation des perturbations en cas de menace.

Autres avantages potentiels : meilleure visibilité, réduction du nombre de périphériques non gérés et non conformes qui accèdent aux systèmes de l'entreprise, accélération de l'application des correctifs, réduction du risque d'échec aux audits, et économies financières. Pour bénéficier de tels avantages, il suffit de se doter des bons outils. Vous obtiendrez à la clé une réduction des interventions manuelles.

6 étapes pour surmonter le dilemme qui freine les entreprises

Même si le tableau que nous venons de brosser est idéal, le cheminement pour y parvenir peut décourager. Au début, vous faites face à un dilemme sans réponse précise. Votre département doit renforcer la sécurité, limiter les menaces, améliorer la productivité et conserver les ressources tout en faisant face à une nouvelle problématique : la dispersion des effectifs et l'extension rapide du paysage des menaces et des surfaces d'attaque empêchent la mise en œuvre de nouvelles stratégies.

C'est pourquoi nous avons défini six étapes pour aider les entreprises à trouver leur voie. Chacune couvre un élément essentiel dans le paysage actuel. Ensemble, ces étapes constituent les bases d'une stratégie de gestion de la cybersécurité complète et évolutive.

Étape 1

Bénéficiez d'une visibilité complète sur l'ensemble des biens

Il est impossible de gérer ce que l'on ne connaît pas. Sans inventaire précis et consolidé de ses ressources Cloud et de ses biens (matériels et logiciels), votre entreprise est vulnérable aux risques de sécurité et s'expose à un manque de conformité, à des procédures de suivi trop complexes et à un manque de fiabilité des données.

Face à la pénurie mondiale de ressources IT, il est temps d'investir dans une plateforme d'automatisation qui utilise au mieux et entièrement les capacités de votre équipe. Une solution de découverte complète trouve tous les biens sur votre réseau, qu'ils soient propriété de l'entreprise ou en BYOD, et les cartographie en contexte. Vous savez ainsi qui utilise quel périphérique, comment et quand cette personne l'utilise pour interagir avec l'entreprise, et quelles sont les ressources auxquelles elle accède.

Avantages de la découverte des biens :

- Obtenir une visibilité complète en temps réel sur l'ensemble des périphériques et logiciels connectés, avec leur contexte
- Mettre en place une gestion, une protection et un service efficaces des biens, partout
- Rationaliser et organiser les données de chaque source
- Suivre et récupérer les licences logicielles
- Optimiser les dépenses globales de biens IT (matériel, logiciels, Cloud)

Fonctionnalités attendues d'une solution de découverte :

- Découverte, gestion et sécurisation des périphériques recensés sur le réseau et en dehors, y compris ceux qui se connectent à des services Cloud.
- Découverte automatique et cartographie (M.A.P.) des relations entre les principaux biens matériels et logiciels, ainsi que les services et applications qui dépendent de ces biens.
- Base de données consolidée de l'ensemble des biens, capable de récupérer les informations de différents systèmes : outils UEM (gestion unifiée des points de terminaison), passerelles réseau, services Cloud et outils ITSM.
- Rapprochement entre les éléments fournis par le département IT et ceux qui se connectent activement aux services de l'entreprise.
- Connecteurs des sources de données (fournisseur, bases de données de contrats, garantie matérielle, etc.).
- Intégration avec les processus ITSM et de sécurité pour une correction proactive des problèmes IT et des vulnérabilités de sécurité.

Étape 2

Modernisez la gestion des périphériques grâce à l'UEM (gestion unifiée des points de terminaison)

Face à l'adoption massive du mode de travail hybride, la sécurité et la gestion des points de terminaison sont au cœur des préoccupations du personnel IT et des collaborateurs. Une gestion moderne des périphériques (MDM) permet de booster la productivité des utilisateurs et du département IT, d'automatiser le provisionnement des périphériques et le déploiement des logiciels, et de résoudre rapidement les problèmes des utilisateurs.

Pour réduire le temps de support et garantir que tous les périphériques sont gérés avec cohérence, choisissez une solution UEM dotée de fonctions de gestion prenant en charge une grande variété de systèmes d'exploitation (iOS, Android, Windows, macOS, Linux, ChromeOS, dispositifs spécialisés des intervenants de première ligne, périphériques IoT et portables) pour assurer à la fois une gestion moderne et une gestion basée sur un client.

La solution UEM doit être disponible à la fois sur site et en mode SaaS pour répondre aux besoins de déploiement de votre entreprise. Grâce à la séparation des données professionnelles et personnelles, la gestion unifiée des points de terminaison préserve la vie privée de vos collaborateurs. L'UEM prend aussi totalement en charge le BYOD, tout en optimisant à la fois la confidentialité des données utilisateur et la sécurisation des données de l'entreprise.

Avantages d'une approche UEM pour gérer les périphériques :

- Gestion et sécurité cohérentes pour tous vos périphériques.
- Facilitation de l'onboarding, du provisionnement des applications et de la configuration des périphériques à l'échelle, ce qui améliore la productivité du département IT et l'expérience des utilisateurs.
- Surveillance de l'état de santé des périphériques et assurance de leur conformité, à tout moment.
- Résolution des problèmes, rapidement et à distance.
- Automatisation des mises à jour logicielles et des déploiements d'OS.
- Amélioration de la prise de décision IT grâce à des tableaux de bord détaillés et des fonctionnalités d'intelligence en temps réel.
- Détection et correction des vulnérabilités de l'OS et des applis tierces.
- Augmentation de la productivité des collaborateurs grâce à la réduction des interruptions et meilleure expérience collaborateur grâce à la rationalisation de l'onboarding.

Fonctionnalités attendues d'une solution de gestion des périphériques :

- Processus d'onboarding simple et provisioning tout aussi simple pour le département IT grâce à des services comme Apple Business Manager (ABM), Google Zero-Touch Enrollment et Windows AutoPilot qui permettent un recensement automatique des périphériques des collaborateurs.
- Découverte, gestion et sécurisation de tous les points de terminaison sous iOS, Android, macOS, Windows, Linux et ChromeOS, ainsi que des périphériques immersifs comme HoloLens, Oculus et Zebra.
- Prise en charge de plusieurs modèles de propriété afin de pouvoir gérer, configurer et sécuriser les périphériques appartenant à l'entreprise, les périphériques en BYOD et les périphériques partagés.
- Capacité à autonomiser les employés en première ligne et à sécuriser les applis métiers sur leurs périphériques sans qu'il soit nécessaire de gérer ces périphériques.
- Mise en place d'un accès sécurisé aux données et applis sur tous les périphériques.
- Visibilité sur l'ensemble des périphériques gérés via des rapports personnalisés et contrôle poussé via des actions correctives automatisées.

Étape 3

Mettez en place une bonne hygiène des périphériques

Pour mettre en place des règles d'hygiène informatique pour vos périphériques, il faut adopter une approche proactive afin de garantir que seuls ceux répondant à des exigences de sécurité définies sont autorisés à accéder aux ressources de l'entreprise. Cela implique d'installer des systèmes capables d'appliquer automatiquement des correctifs aux périphériques ou de mettre en quarantaine ceux comportant des vulnérabilités logicielles au niveau du système d'exploitation et des applications. Une bonne hygiène informatique exige de choisir des solutions de bonne réputation afin de réduire la surface d'attaque.

Une mauvaise hygiène des périphériques, au contraire, peut rendre votre entreprise vulnérable aux cyberattaques, notamment aux ransomwares. Dans ce cas, c'est au département IT (et non à des solutions spécialement conçues) qu'il incombe de suivre activement les vulnérabilités et de protéger l'entreprise des cyberattaques.

Hygiène des périphériques mobiles

Bien que 71 % des professionnels considèrent que les périphériques mobiles sont indispensables dans leur vie professionnelle, les responsables de sécurité sont presque tous d'accord : les télétravailleurs sont exposés à davantage de risques que les personnes travaillant au bureau.

Et pourtant, 3 professionnels de la sécurité sur 4 ont succombé à la pression, et sacrifié la sécurité des périphériques mobiles par convenance personnelle.[6]

C'est un vrai problème. L'hygiène des périphériques mobiles doit être irréprochable pour combattre les vulnérabilités auxquelles ils sont exposés (jailbreak, détection root, versions d'OS vulnérables, etc.), les vulnérabilités du réseau (attaques « Man-In-The-Middle », point d'accès malveillants, Wi-Fi non sécurisé, etc.) et les vulnérabilités des applications (évaluation des risques de sécurité élevés, évaluation des risques de confidentialité élevés, comportement suspect des applis, chargement latéral d'applications, etc.).

Avantages de la mise en place d'une bonne hygiène des périphériques mobiles :

- Réduction des erreurs humaines et de l'investissement IT grâce à une intelligence automatisée basée sur les risques.
- Détection et élimination des vulnérabilités Zero Day pour ne plus avoir à s'inquiéter du futur.
- Détection et résolution des problèmes même sur des périphériques éteints ou non connectés.
- Préservation de vos données, de vos ressources et de votre marque grâce à une surface d'attaque réduite.

Fonctionnalités attendues d'une solution de MTD (protection contre les menaces mobiles) :

- Favorisez les logiciels capables de vous protéger contre tous les types d'attaques mobiles, y compris l'hameçonnage et les attaques au niveau du périphérique, du réseau et des applications.
- La protection des périphériques Android ET des périphériques iOS est essentielle. Choisissez une application unique dotée d'un moteur de Machine Learning sur le périphérique, associé à un client UEM. Les utilisateurs sont bien plus enclins à adopter une application unique que plusieurs.
- Optez de préférence pour une solution assurant une protection multiniveau afin de vous prémunir contre les menaces au niveau du périphérique, du réseau et des applications (en plus de l'antihameçonnage), et dotée de fonctionnalités de détection des menaces à la fois sur le périphérique et dans le Cloud. La protection sur le périphérique n'a pas besoin de connexion Internet pour continuer à détecter et à éliminer les menaces.
- Il est indispensable d'appliquer une stratégie de mise en conformité multiniveau, pouvant servir à alerter l'utilisateur final et l'administrateur si le périphérique n'est pas conforme. En cas de non-conformité, le système réagit avec des mesures de plus en plus sévères, du blocage de l'accès à la ressource d'entreprise à la mise en quarantaine, jusqu'au retrait du périphérique et à la suppression de la totalité des applis, du contenu, des paramètres, etc. provisionnés par l'UEM.

Hygiène des postes de travail/ordinateurs portables

Tant que les attaques par rançongiciel et autres fuites de données ne sont pas révolues, les entreprises doivent prendre des mesures pour s'en protéger. Ainsi, l'application de correctifs pour éliminer les CVE (Common Vulnerabilities and Exposures - la liste publique des vulnérabilités et failles de sécurité) est l'une des meilleures mesures qu'une entreprise peut prendre pour bloquer les attaques par ransomware. Malheureusement, une étude Ivanti[7] montre que 71 % des professionnels de l'IT et de la sécurité considèrent que l'application des correctifs est trop complexe et trop longue. Cela peut s'expliquer par le volume effarant de vulnérabilités que l'on connaît.

Aux États-Unis, la base de données nationale des vulnérabilités (NVD) répertorie plus de 100 000 vulnérabilités. Bien que seul un faible pourcentage de ces vulnérabilités soit lié au ransomware, et que le pourcentage d'exploitations actives soit encore plus faible, il est parfois difficile pour une entreprise d'identifier les menaces les plus dangereuses. Un rapport Ivanti montre[8] que sur 2018-2020, d'après les scores CVSS v3, les entreprises ayant uniquement appliqué les correctifs de vulnérabilités « critiques » n'étaient protégées que contre 35 % des ransomwares. Une application automatisée des correctifs sur la base des risques est indispensable à l'hygiène des postes de travail/ordinateurs portables.

Avantages de la mise en place d'une bonne hygiène des postes de travail/ordinateurs portables :

- Comme pour les périphériques mobiles, il s'agit de limiter les erreurs humaines et l'investissement IT grâce à une intelligence automatisée basée sur les risques.
- Limitation des probabilités d'attaque par rançongiciel grâce à l'application des correctifs pour corriger les CVE sur la base des risques réellement encourus.
- Avec la priorisation automatisée des menaces, vous appliquez les correctifs de façon stratégique et optimisez l'allocation des ressources.
- Grâce à l'automatisation, vous êtes en mesure de contrer des menaces sans dépendre des interventions humaines.

Fonctionnalités attendues d'une solution d'hygiène des postes de travail/ordinateurs portables :

- Sur les postes de travail/ordinateurs portables, il est essentiel de mettre régulièrement à jour les logiciels afin d'éradiquer (ou, au moins, de limiter) les vulnérabilités. Comme l'application des correctifs peut devenir très complexe, choisissez de préférence une solution capable d'évaluer automatiquement les risques et de fournir des informations utiles, en donnant la priorité aux vulnérabilités les plus pressantes.
- La priorisation basée sur les risques procure une meilleure visibilité sur les faiblesses les plus dangereuses au sein de votre environnement. L'entreprise peut ainsi cibler les correctifs les plus critiques. Essentiel pour les départements IT et Sécurité, le contexte des menaces actives (mise en correspondance des vulnérabilités avec les informations fondées sur des menaces réelles) permet de prioriser l'application des correctifs afin de contrer les menaces les plus dommageables.

Étape 4

Sécurisez vos utilisateurs

Les seules personnes à aimer les mots de passe sont les pirates, parce qu'ils s'en servent pour attaquer. Lourde pour les utilisateurs, l'authentification par mot de passe ne contextualise pas le périphérique, l'application, le réseau ou les menaces. Comment savoir qui saisit le mot de passe ? Est-ce bien un collaborateur ou s'agit-il d'un pirate qui le lui a volé ? Même les mots de passe les plus complexes peuvent être craqués assez facilement via une attaque par force brute, par hameçonnage ou autre.

Les données d'identification, comme les mots de passe, restent les plus recherchées. On les retrouve dans 61 % des fuites[9]. Compromises plus rapidement que tout autre type de données, elles sont la cible privilégiée des tentatives d'hameçonnage, qui cherchent une porte d'entrée dans l'entreprise.

Les solutions SSO (identification unique) créent un point de défaillance unique, que les pirates peuvent exploiter pour accéder à la plupart des applis d'une entreprise, voire à toutes. D'après une étude[10], 42 % des collaborateurs réutilisent un même mot de passe pour plusieurs comptes, et 17 % alternent deux à cinq mots de passe. Ainsi, si un collaborateur se fait pirater un compte hors du cadre professionnel, mais se sert du même mot de passe au travail, votre entreprise est en danger.

Avec l'essor du télétravail, on pourrait penser que les entreprises ont renforcé leurs protocoles de mot de passe, mais une étude Verizon[11] montre que dans plus d'un tiers des cas, les règles d'authentification se sont assouplies pour s'adapter aux restrictions de la crise sanitaire.

Il est temps de choisir l'authentification sans mot de passe avec le Zero Sign-On.

Le Zero Sign-On est une méthode d'authentification qui n'utilise aucun mot de passe, de même que le Single Sign-On n'en utilise qu'un seul.

L'authentification sans mot de passe sécurise vos collaborateurs, avec les avantages suivants :

- Aucun mot de passe = aucune donnée d'authentification à voler ou à hameçonner.
- Aucun mot de passe = satisfaction accrue des utilisateurs, qui n'ont pas à mémoriser les mots de passe et ne risquent pas de bloquer leur compte.
- Progression du niveau de maturité de votre sécurité Zero Trust.
- Baisse des coûts avec la disparition de la gestion des réinitialisations et des fuites de mot de passe.

> "Il est impossible de savoir qui saisit le mot de passe : est-ce bien un collaborateur ou s'agit-il d'un pirate qui le lui a volé ?"

Fonctionnalités attendues d'une solution d'authentification :

- La solution idéale permet d'accéder sans mot de passe aux périphériques, aux applis métier et aux services Cloud.
- Pour être efficace, l'accès sans mot de passe repose sur l'authentification multifacteur (MFA) qui vérifie un facteur matériel en votre possession (par exemple un périphérique mobile) ; un facteur corporel d'ordre biométrique (empreinte digitale, reconnaissance faciale) ; et le contexte (lieu, heure du jour) qui remplace le facteur mémoriel (mot de passe, questions de sécurité).
- Dans une démarche de sécurité Zero Trust avec accès contextuel, choisissez une solution qui s'intègre avec une solution de gestion unifiée des points de terminaison (UEM) pour contrôler les utilisateurs, les périphériques, les applications, le réseau et les menaces avant d'accorder tout accès.
- Recherchez une solution d'authentification sans mot de passe qui s'intègre sans difficulté avec vos solutions existantes, notamment IdP/IAM, MTD/XDR/EDR, SOAR, SIEM.

Étape 5

Fournissez un accès sécurisé

Les périmètres réseau utiles pour des effectifs sur site ne suffisent plus dans l'Everywhere Workplace du télétravail. Vos collaborateurs travaillent désormais depuis n'importe où et souvent de lieux inattendus : pour s'adapter à cette évolution, votre périmètre réseau actuel doit lever les limitations et les complexités, non sans garantir la sécurité.

Les réseaux d'aujourd'hui doivent être construits sur le principe de périmètre défini par logiciel (SDP). Un SDP fournit une architecture de sécurité intégrée, difficile à obtenir avec les produits de sécurité existants comme les antimalwares. Il s'appuie sur des composants normalisés ayant fait leurs preuves, comme le chiffrement des données, l'attestation à distance, l'authentification Mutual TLS et le langage SAML. L'incorporation de ces technologies et d'autres basées sur les normes garantit la bonne intégration du SDP à vos systèmes de sécurité existants.

Si le SDP est une structure réseau, la couche de sécurité reste indispensable pour en tirer tous les avantages. C'est là qu'intervient le Zero Trust, et plus précisément le ZTNA, l'accès réseau sans confiance. Gartner définit le ZTNA comme un produit ou service qui dresse autour d'une application ou d'un groupe d'applications une barrière d'accès logique en fonction de l'identité et du contexte. Le SDP peut servir à implémenter des réseaux Zero Trust.

Avantages de l'accès sécurisé généralisé :

- Seuls les utilisateurs de confiance authentifiés ont accès aux ressources.
- Un périmètre extérieur du réseau est plus malléable avec à la clé des déploiements plus flexibles et des workflows plus faciles pour vos collaborateurs.
- Fin des limitations et de la complexité des périmètres stricts, il est désormais inutile d'ouvrir des accès supplémentaires vers des sous-sections du réseau.
- Sécurité et visibilité préservées avec un accès facilité.

Fonctionnalités attendues d'une solution de réseau Zero Trust :

- Souveraineté des données : les données applicatives ne transitent pas sur le réseau d'un fournisseur et ne sont pas exposées à Internet. Ce chemin direct optimise les performances et l'expérience des utilisateurs.
- Visibilité globale : activité par utilisateur, par périphérique et par application, y compris pour les ressources déployées en mode SaaS.
- Évaluation adaptative en continu de l'approche sécuritaire du client, avec application automatisée de règles en fonction d'éléments fluctuants (comportement, lieu).

Étape 6

Gérez la conformité et les risques

La démarche de conformité et d'atténuation des menaces impose de maîtriser la gouvernance, la gestion des risques et la conformité (GRC).

Trop souvent, les entreprises gèrent la conformité manuellement… et dans des feuilles de calcul. Incroyable, non ? Elles dépensent souvent des budgets énormes dans des produits de sécurité disparates, sans vraiment comprendre comment les intégrer et les exploiter. On pourrait dire à l'aveuglette.

L'exposition aux risques doit s'envisager dans sa globalité. Hélas, les évaluations des postures sécuritaires, pour la plupart après un incident, se limitent au vecteur de l'attaque. Associée au manque de personnel IT, cette approche réactive est vraiment problématique.

> "Trop souvent, les entreprises gèrent la conformité manuellement… et dans des feuilles de calcul. Incroyable, non ?"

Avantages d'une bonne compréhension de la conformité et des risques :

- Des processus de conformité automatisés à la place de tâches manuelles.
- Des audits bien préparés qui se déroulent mieux.
- Atténuation des risques en amont.
- Budget aligné sur les risques réels et non supposés.
- Framework de conformité plus fiable et plus axé sur la stratégie.
- Adaptation aux constantes évolutions réglementaires sans intervention des développeurs.
- Collaborateurs déchargés et réaffectés à des tâches plus stratégiques.

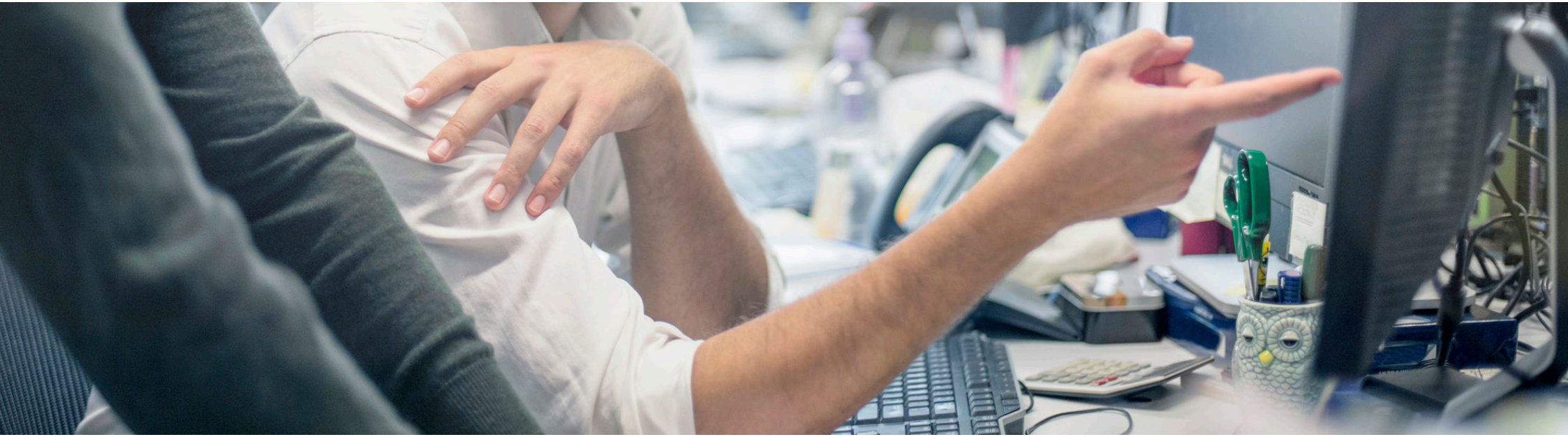
Fonctionnalités attendues d'une solution de mise en conformité :

- Une solution robuste facilite les tâches de conformité par l'importation rapide et simple de documents réglementaires pour faire correspondre votre parcours M.A.P. avec les contrôles de sécurité et de conformité.
- La capacité de gestion proactive des risques implique de focaliser son attention au bon endroit au bon moment.
- L'objectif est d'automatiser les tâches manuelles répétitives de gouvernance pour une conformité sans accroc.
- La gestion de la maturité des processus vous permet d'évaluer la maturité de vos processus et contrôles de sécurité critiques, et de les optimiser en fonction des priorités et des risques.
- Pour des résultats efficaces et précis, privilégiez une solution qui vous guide tout au long de l'évaluation des risques.

Tracez votre parcours de cybersécurité (M.A.P.)

Chacune de ces six étapes est essentielle pour gérer, automatiser et prioriser votre parcours de cybersécurité. Vous vous sentez dépassé par l'ampleur de la tâche ? Vous ne savez pas par où commencer ? Faites-vous accompagner par des partenaires et adoptez des solutions qui vous aideront tout au long de votre parcours. Avec des solutions complètes et intégrées, vos équipes verront leur charge de travail allégée. De plus, ces solutions de pointe procurent une expérience utilisateur productive et intuitive, véritable vecteur d'intégrité, quel que soit l'endroit, le moment ou la façon dont vos collaborateurs travaillent

Travailler de partout en toute sécurité.



À propos d'Ivanti

Ivanti rend possible l'Everywhere Workplace. Dans l'Everywhere Workplace, les collaborateurs utilisent une multitude de périphériques pour accéder aux données et aux applications du département IT sur différents réseaux, afin de rester productifs en travaillant de partout. La plateforme d'automatisation Ivanti Neurons connecte les solutions Ivanti de gestion unifiée des terminaux (UEM), de sécurité Zero Trust et de gestion des services d'entreprise (ESM), leaders du marché, afin de créer une plateforme IT unifiée permettant l'autoréparation et l'autosécurisation des périphériques, et le self-service aux utilisateurs. Plus de 40 000 clients, dont 96 des entreprises Fortune 100, ont choisi Ivanti pour découvrir, gérer, sécuriser et servir leurs biens IT, du Cloud à la périphérie, ainsi que pour fournir une expérience utilisateur d'excellence aux collaborateurs, où qu'ils se trouvent et quelle que soit la façon dont ils travaillent. Pour en savoir plus, visitez le site ivanti.fr

ivanti

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

1. Une enquête Gartner révèle que 82 % des responsables d'entreprise prévoient d'autoriser leurs collaborateurs à télétravailler, au moins à temps partiel
2. Ivanti: Patch Management Challenges. https://www.ivanti.com/resources/v/doc/datasheets/ivi-2634-patch-management-challenges
3. Statista: Global average cost of a data breach 2021.
4. Statista: Average https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/ length of downtime after a ransomware attack 2021.
5. The biggest data breach fines, penalties, and settlements so far | CSO Online
6. 2021 Data Breach Investigations Report | Verizon
7. https://www.ivanti.com/resources/v/doc/datasheets/ivi-2634-patch-management-challenges
8. https://www.ivanti.com/resources/v/doc/white-papers/spotlight_ransomware2021_risksensecsw?_ga=2.114312003.538830105.1638796042-898995573.1638285247
9. 2021 Data Breach Investigations Report | Verizon
10. Best Password Managers 2021 | The Strategist (nymag.com)
11. People and behaviors | Verizon