jamf

Le playbook des technologies émergentes : gestion, sécurité et croissance de l'entreprise moderne

Les technologies mobiles émergentes en entreprise

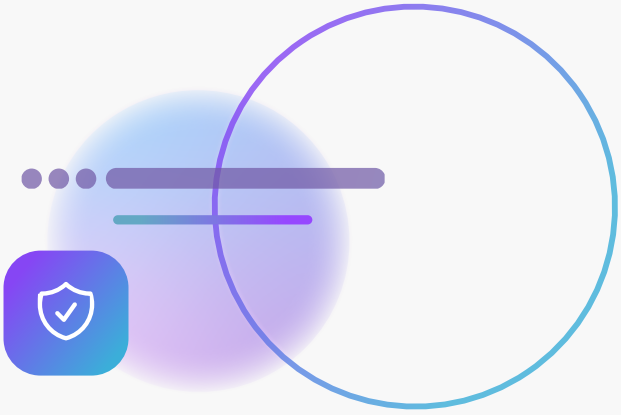
Tout comme les espaces de travail ont évolué là, les technologies émergentes, comme les dispositifs corporels, l'informatique spatiale et l'IA, modifient les pratiques et les méthodes. Dans l'entreprise, elles améliorent l'expérience des utilisateurs, dopent la productivité et accélèrent l'innovation, dans tous les secteurs et toutes les régions du monde.

Pour suivre le rythme de ces mutations, les dirigeants et les équipes informatiques et de sécurité doivent faire évoluer leurs stratégies en matière de terminaux pour remplir leur mission : sécuriser les données, assurer une gestion complète des appareils, et accompagner la croissance de l'entreprise en atténuant les risques liés à l'élargissement des surfaces d'attaque, à la fragmentation de la visibilité et à l'intensification de la demande en ressources opérationnelles.

En plus d'exposer les raisons pour lesquelles les organisations ont tout intérêt à moderniser leur gestion, ce document fournit des conseils pour développer, indépendamment des plateformes, un socle résilient basé sur un contexte réel et des actions concrètes dans un triple objectif : réduire la complexité, combler les lacunes de visibilité et se préparer à l'ère de l'informatique hybride.

Dans ce document, vous apprendrez à :

- Adapter les stratégies de gestion et de conformité aux technologies émergentes.
- Identifier les raisons qui empêchent les approches traditionnelles d'assurer une sécurité homogène.
- Intégrer l'automatisation et l'application continue des règles à vos stratégies de base.
- Aligner la gestion, l'identité, la sécurité et la conformité sur les objectifs de l'entreprise.
- Adopter l'approche « zero trust » comme principe de base de la sécurité des terminaux modernes.



Synthèse

Les entreprises entrent dans une ère caractérisée par des avancées rapides dans les modèles informatiques hybrides, et notamment dans le domaine des dispositifs corporels, de l'IoT et de l'IA. Ces technologies émergentes transforment les opérations et stimulent l'innovation dans tous les secteurs, mais elles sont également source de complexité, de fragmentation et de risques. La diversité croissante des parcs d'appareils exige une gestion holistique, des règles d'accès contextualisées, une validation continue de la posture et l'adoption d'une approche « zero trust ». En investissant dans des workflows automatisés, une visibilité approfondie et des contrôles axés sur des règles, les organisations auront toutes les cartes en main pour protéger leurs données, répondre à l'évolution des réglementations et déployer des technologies émergentes avec assurance.

Les points clés à retenir :

- Projection du TCAC des appareils renforcés d'ici 2028 : **8,4 %**
- Projection du TCAC de l'informatique spatiale d'ici 2030 : **33,16 %.**
- Adoption en entreprise de paradigmes informatiques hybrides d'ici 2028 : **40 %.**
- Problèmes de service à la clientèle résolus de manière autonome d'ici à 2029 : **80 %.**
- Prédiction des ventes de dispositifs corporels en 2025 : **590,7 millions d'unités**

Technologies émergentes : 2026 et au-delà

Une nouvelle ère de l'informatique est en train de s'ouvrir : les dispositifs corporels, l'IoT et l'IA passent du stade des programmes pilotes à celui d'outils d'entreprise capables de produire des résultats commerciaux. Ces technologies remodèlent la façon dont les gens travaillent, apprennent et échangent, en estompant la frontière entre notre monde physique et nos espaces de travail numériques. Grâce à elles, nous atteignons des niveaux inédits de créativité, de productivité, de collaboration, de perspicacité et d'automatisation. Les organisations qui sauront s'emparer de cette dynamique vont renforcer leur alignement stratégique et leur résilience, évoluer intelligemment et saisir les opportunités de la prochaine vague d'innovation.

Informatique spatiale

Le jeu en réalité virtuelle (VR) Vortex, que l'on pouvait voir dans certaines salles d'arcade à la fin des années 90, a été pour beaucoup la première incursion dans les expériences de réalité alternative. Cette technologie, qui englobe la réalité augmentée (AR) et la réalité étendue (XR), a évolué pour devenir la réalité mixte (MR) qui jette un pont entre mondes physique et logique pour nous aider à les comprendre.

Appelée « informatique spatiale », elle incarne la prochaine évolution de l'apprentissage et de la productivité, avec **un taux de croissance annuel composé (TCAC) estimé à 33,16 % d'ici 2030**.

Bien que l'informatique spatiale n'en soit qu'à ses débuts, l'influence de cette technologie **est sensible dans de nombreux secteurs à l'échelle mondiale**, et en particulier dans l'éducation, la fabrication et la santé, entre autres.

Quelques exemples d'applications concrètes de l'informatique spatiale :

- **Onboarding simplifié :** les employés se familiarisent avec leur nouvelle entreprise en explorant les locaux pour trouver leurs marques dès le premier jour.
- **Prototypage rapide :** les ingénieurs développent des produits et génèrent des itérations plus rapidement grâce aux outils de manipulation permettant de tester leur intégrité et à la collaboration en temps réel.
- **Formation spécialisée :** les chirurgiens s'exercent dans un environnement réaliste, et les superpositions 3D permettent de créer une simulation immersive pour apprendre de nouvelles procédures et gagner en précision.
- **Expériences enrichies :** dans le commerce de détail, les clients utilisent leur smartphone pour scanner des objets, visualiser des produits ou essayer des vêtements à domicile.
- **Dépannage juste à temps :** les opérateurs de machines utilisent l'Apple Vision Pro pour identifier et analyser les problèmes afin de les résoudre dans l'atelier de production.

Dispositifs corporels

Imaginez : sous une forme miniaturisée, une Apple Watch contient des composants matériels autrefois réservés aux ordinateurs de bureau de classe Pentium 4.

Grâce au traitement multicœur, aux moteurs neuronaux, à toute une série de capteurs microscopiques et à une capacité de calcul autonome, il est aujourd'hui possible de combiner travail et loisirs dans un design performant et économe en énergie, attaché à votre poignet, votre main ou même votre doigt.

Voici quelques applications des **590,7 millions de dispositifs corporels vendus en 2025** :

- **Montres :** simplifiez vos déplacements dans le monde entier avec une montre connectée compatible GPS et cellulaire pour rester en communication avec le bureau et vos proches sans vous inquiéter des complexités et des frais associés à l'itinérance.
- **Traqueurs :** obtenez des informations de santé et des signes vitaux en temps réel pour suivre vos objectifs ou réagir rapidement en cas d'incident et recevoir des soins sans délai.
- **Écouteurs :** la technologie de réduction du bruit limite les distractions extérieures pour faciliter la concentration. Jumelés à un smartphone, les écouteurs peuvent traduire en direct plusieurs langues parlées en temps réel.
- **Lunettes :** prenez des photos et des vidéos, et répondez à des messages urgents tout en suivant des indications pour vous rendre à votre rendez-vous, tout cela en mode mains libres grâce à l'assistant IA intégré.

Internet des objets (IoT)

L'efficacité est un moteur de continuité des activités. Et comme l'automatisation est cruciale pour l'efficacité, il n'est pas surprenant que les appareils IoT soient largement utilisés pour produire de la business intelligence. Les flux de processus, notamment, sont essentiels pour prendre des décisions axées sur les données afin de simplifier les opérations commerciales à grande échelle.

Dans certains cas, la combinaison de capteurs et de l'automatisation permet de réaliser des **économies de coûts énergétiques d'environ 20 à 30 %**. Certaines entreprises enregistrent une **réduction des coûts de maintenance pouvant aller jusqu'à 50 %** grâce à des stratégies telles que la maintenance prédictive, qui réduit les temps d'arrêt non planifiés en favorisant une approche proactive.

Quelques exemples qui illustrent l'intérêt de l'IoT en entreprise :

- **Suivi des actifs et réseau logistique :** simplifiez le suivi des inventaires et améliorez la planification des capacités et la prévision des stocks en y associant l'analyse prédictive.
- **Personnalisation de l'expérience client :** fidélisez votre base de clients en proposant des interactions personnalisées en phase avec leurs besoins, tout en améliorant la prestation de services.
- **Gestion des bâtiments et des installations :** réduisez l'empreinte énergétique tout en augmentant l'efficacité des bâtiments en automatisant les fonctions CVC, l'éclairage et la sécurité.
- **Interconnexion des systèmes sophistiqués :** maximisez la valeur des systèmes existants en y intégrant des capteurs et l'IoT pour offrir de nouveaux services et créer de nouvelles opportunités de revenus.

Intelligence artificielle (IA)

Les promesses de l'IA concernent aussi bien les entreprises que les utilisateurs. Les applications de l'IA générative concernent tous les secteurs, dans le monde entier, et son pouvoir de transformation semble illimité :

- **Valeur ajoutée accrue :** lorsque les tâches répétitives sont exécutées automatiquement, les employés sont libres de consacrer leurs compétences à des activités stratégiques.
- **Augmentation du ROI :** une meilleure utilisation des ressources et des gains d'efficacité permettent d'optimiser les processus et de réduire les coûts d'exploitation, tout en offrant des avantages qualitatifs liés à l'innovation et à l'amélioration de l'expérience client.
- **Simplification des processus :** maximisez les ressources en visualisant les concepts, en résumant des contenus ou en développant rapidement des éléments de code.
- **Analyse amplifiée :** obtenez des renseignements ciblés, évaluez les tendances et prenez des décisions proactives basées sur les données afin de réduire les délais de commercialisation (GTM).

À tout cela s'ajoutent aujourd'hui les bénéfices de l'IA agentique, capable de prendre des décisions sans interaction humaine. Par exemple, une étude de Gartner estime que **80 % des problèmes courants soumis au service client seront résolus de manière autonome d'ici 2029**. Ses capacités de proaction (recherche des menaces) et d'adaptation (apprentissage en temps réel) s'annoncent également très prometteuses. Dans le domaine des logiciels de cybersécurité, en particulier, elle est sur le point de révolutionner des processus cruciaux des entreprises. Les solutions de sécurité exploitant l'IA agentique surveillent et évaluent en permanence les facteurs de risque ; elles prennent des mesures pour atténuer les menaces rapidement, sans intervention humaine, afin de réduire les temps de réponse et de maintenir la résilience.

Informatique hybride

Les entreprises du monde entier sont confrontées à des défis d'efficacité, de gestion des charges de travail, de provisionnement en ressources et de croissance, auxquels s'ajoutent des obligations réglementaires et des dépenses d'investissement. Dans ce nouveau contexte, les modèles informatiques traditionnels – systèmes locaux, clouds publics/privés – ne sont plus à la hauteur des enjeux. Même les modèles à faible latence comme l'edge computing, qui rapproche le traitement des données de l'appareil pour accélérer l'exécution, ne répondent pas encore à toutes les questions soulevées par l'évolution rapide du paysage numérique.

Le nouveau paradigme de l'informatique hybride englobe à la fois les technologies et les modèles informatiques existants pour surmonter les obstacles évoqués :

- **Agilité** : miser sur plusieurs modèles informatiques permet aux organisations d'optimiser le traitement du trafic, de façon à réduire les temps de réponse et la latence à peu de frais pendant les périodes de pointe inattendues.
- **Performance** : en distribuant intelligemment les charges de travail dans l'environnement le plus efficace, les outils pilotés par l'IA et l'automatisation offrent d'importants gains de productivité.
- **Conformité** : la géopatriation donne aux organisations du contrôle sur la résidence des données et des applications, ce qui garantit la souveraineté et la conformité aux lois sur la protection de la vie privée et aux réglementations.
- **Résilience** : une continuité rationalisée assure le maintien des opérations commerciales pendant les pannes grâce à l'intégration des systèmes cloud, sur site et traditionnels.

D'ici 2028, Gartner prévoit que **plus de 40 % des grandes entreprises auront adopté des architectures informatiques hybrides** pour les workflows critiques de l'entreprise, contre 8 % actuellement.

Les défis pour le service informatique des entreprises

Lorsque les appareils quittent le périmètre de la gestion, la visibilité est entravée et il devient plus difficile de :

- Évaluer les postures de sécurité
- Réagir rapidement aux menaces
- Maintenir la sécurité des données

La diversité des plateformes, des appareils et des modèles de propriété, conjuguée aux environnements de travail hybrides, introduit des variables qui élargissent la surface d'attaque d'une organisation. Elle exerce également une pression supplémentaire sur les équipes chargées d'atténuer les risques posés par les mutations des menaces. Dans un contexte d'évolution des réglementations et de fragmentation des standards de l'IA et de l'IoT, la gouvernance et l'éthique de l'IA deviennent des enjeux majeurs pour les organisations du monde entier et les secteurs dans lesquels elles opèrent.

Inscription et provisionnement

Une stratégie complète de gestion et de sécurité commence par l'inscription des appareils. C'est elle qui permet ensuite de doter les appareils des outils et des configurations nécessaires pour assurer la conformité des organisations, la protection des données et la productivité des employés. Cette bonne pratique est au cœur de workflows informatiques holistiques et bénéficie de nombreux standards et cadres de déploiement.

Lorsque les appareils ne sont pas inscrits dans une solution de gestion ni équipés des outils professionnels indispensables, les implications néfastes sont multiples et dégradent notamment :

- la convivialité des appareils
- la confidentialité des données
- l'intégrité des communications
- la confidentialité des utilisateurs
- la disponibilité des points de terminaison

Chaque facteur de risque pèse sur la fourniture des services et la conformité réglementaire, avec des effets en cascade sur la continuité des activités.

Des lacunes dans la visibilité et l'application des règles

Les informations sur les appareils constituent la pierre angulaire de toute stratégie de sécurité. Lorsqu'elles sont dans l'impossibilité de visualiser et d'analyser l'état de santé des terminaux, les équipes informatiques et de sécurité sont privées d'informations sur les activités des appareils qui se connectent à l'infrastructure, communiquent, demandent des ressources de l'entreprise et les utilisent.

Ces angles morts dans la télémétrie peuvent empêcher les administrateurs d'atténuer toute une série de problèmes, parce qu'ils manquent de visibilité sur les menaces et ne savent pas quelles ressources protéger en priorité en cas d'urgence.

Voici quelques facteurs courants de visibilité dégradée :

- Pluralité des systèmes d'exploitation
- Altération physique des appareils
- Modèles de propriété mixtes
- Types d'appareils non pris en charge
- Défauts dans la configuration des appareils

Atténuation des menaces et des risques

Les équipes de cybersécurité le savent bien, les acteurs malveillants ciblent depuis longtemps le matériel et les logiciels à la recherche de points d'entrée. Mais aujourd'hui, le défi de la réduction des risques est amplifié par les environnements hybrides et la diversité des appareils et des OS, sources de nouvelles menaces pour l'organisation.

Cette combinaison de systèmes et d'appareils open source, propriétaires et fermés met à rude épreuve les équipes informatiques et de sécurité chargées de gérer et de sécuriser les points de terminaison. Le manque de visibilité sur l'état des terminaux et l'impossibilité d'appliquer des configurations réellement sécurisées à tous les appareils du parc s'ajoutent aux nombreux défis qui entravent déjà les efforts de sécurisation des ressources :

- Sécurité des données
- Exploitation des vulnérabilités
- Résilience du réseau
- Gestion des correctifs
- Élargissement de la surface d'attaque

Exigences réglementaires et conformité

Contrairement aux systèmes traditionnels, les technologies émergentes introduisent une multiplicité de difficultés qui évoluent rapidement. Dans certains cas, comme l'illustre la fragmentation des technologies d'IoT, l'absence de norme unifiée soulève de nombreuses questions en matière de sécurité des données. Dans le domaine de l'IA, beaucoup s'accordent sur les avantages immédiats de la technologie, mais rares sont ceux qui semblent comprendre ses implications pour l'humanité ou l'environnement, et on est bien loin d'un consensus à ce sujet.

Une grande part de ces préoccupations est résolue en temps réel. Les lois rattrapent la technologie pour protéger les données : la Loi de Californie sur la protection de la vie privée des consommateurs (CCPA) et, en Europe, le Règlement général de protection des données (RGPD) mettent l'utilisation des technologies émergentes sous étroite surveillance. D'autres aspects méritent une évaluation méthodique de la part des dirigeants d'entreprise pour encadrer leur usage :

- Résidence des données
- Résilience opérationnelle
- Gestion des risques liés aux tiers
- Problématiques de gouvernance
- Considérations éthiques

Solutions et bonnes pratiques d'avenir

Pour relever les défis liés à l'adoption des technologies émergentes, les entreprises ont tout intérêt à miser sur des bonnes pratiques éprouvées afin d'optimiser la réduction des risques. Cette approche rigoureuse est gage d'une gestion évolutive et résiliente des points de terminaison au fil de la diversification du parc et de l'évolution des cas d'utilisation en réponse aux nouveaux besoins des entreprises.

Inventaire des points de terminaison

Pour évaluer les risques de manière exhaustive, une entreprise doit d'abord avoir une image nette de son infrastructure. Et la meilleure façon de dresser un tableau de la situation est de procéder à un inventaire complet du matériel, des logiciels, des services et des processus. L'objectif est d'avoir une vision claire :

- de chaque appareil,
- de ses dépendances,
- des workflows et des règles.

En identifiant chaque composant et ses interconnexions, on obtient une vision globale de l'infrastructure, de la manière dont elle communique et avec quels appareils. Et cette vision offre aux entreprises une base solide pour la mise en œuvre de solutions d'avenir.

Évaluation des risques

L'étape suivante consiste à évaluer les facteurs de risque afin de déterminer s'ils sont critiques. Au cours de cette phase, l'objectif n'est pas seulement de réduire les risques, mais d'évaluer la tolérance de l'organisation à l'égard de chacun d'eux.

L'utilisation combinée de méthodes qualitatives et quantitatives permet d'obtenir un indice de cyber-risque qui donne aux décideurs une vue d'ensemble de la situation, étayée par des données et basée sur des indicateurs d'attaques clés :

- **Vecteurs** : chemin emprunté ou méthode utilisée pour exécuter une attaque ou compromettre un système.
- **Complexité** : compétences et ressources nécessaires à un adversaire pour exploiter une faiblesse.
- **Impact** : conséquences commerciales et opérationnelles d'une attaque réussie.
- **Exposition** : faiblesses et lacunes qui exposent un environnement à une exploitation.
- **Gravité :** combinaison de la probabilité de matérialisation d'une menace et de l'ampleur des dommages qu'elle pourrait causer.
- **Correction** : existence d'un correctif, nature et rapidité avec laquelle il peut être déployé.

Modélisation des risques

La troisième étape, axée sur la prévention, vise à identifier et à hiérarchiser les risques liés aux appareils, aux systèmes et aux applications. Plus précisément, la modélisation des menaces permet de hiérarchiser les risques par ordre décroissant gravité, avant de procéder aux tests d'intrusion (nous en parlons plus en détail dans la section suivante). Cela permet non seulement de réduire les risques liés aux appareils, mais aussi de renforcer la posture de sécurité de l'organisation.

Différents modèles de menaces permettent d'évaluer des types de risques spécifiques, mais l'on peut également miser sur une approche intégrée pour trouver et quantifier systématiquement les menaces. Quoi qu'il en soit, la meilleure façon de repousser un adversaire est de penser comme lui.

On recense plusieurs méthodes courantes de modélisation des menaces, qui ont chacune leur usage :

STRIDE :
Usurpation (« spoofing »), falsification, répudiation, divulgation d'informations, déni de service et élévation de privilèges.
FONCTION :
Ce modèle classe les risques en fonction de leurs performances dans les six catégories mentionnées.

DREAD :
Pouvoir de nuisance, reproductibilité, exploitabilité, utilisateurs concernés et découvrabilité.
FONCTION :
Ce modèle produit un score moyen basé sur cinq facteurs pour classer la gravité du risque. Il est souvent utilisé de concert avec STRIDE pour prioriser l'atténuation des menaces à haut risque.

LINDDUN :
Liaison, identification, non-répudiation, détection, divulgation des données, ignorance et non-conformité.
FONCTION :
Ce modèle fournit une méthode structurée pour identifier et atténuer les menaces liées à la protection de la vie privée ; il analyse pour cela la circulation des données au sein des applications et des systèmes.

PASTA :
Processus de simulation d'attaques et d'analyse des menaces.
FONCTION :
Ce modèle se concentre sur l'impact des risques pour les entreprises et prescrit des exigences techniques (p. ex. définition des objectifs et du périmètre, analyse des vulnérabilités et simulation d'attaques) pour l'élaboration de stratégies d'atténuation des risques.

OCTAVE :
Évaluation des menaces, des actifs et des vulnérabilités critiques sur le plan opérationnel.
FONCTION : Ce modèle cible, lui aussi, les risques commerciaux afin d'aligner la cybersécurité sur les objectifs de l'entreprise en trois phases : l'élaboration de profils de menaces basés sur les actifs, l'identification des vulnérabilités de l'infrastructure et l'élaboration de stratégies de gestion des risques.

Tests de pénétration

Souvent réalisé pour détecter et hiérarchiser les vulnérabilités des appareils et des logiciels, le test de pénétration, ou « pentest » est sans doute l'exercice d'évaluation des risques le plus courant. Il s'inscrit directement dans la lignée de la modélisation des menaces. Lorsqu'il est effectué après cette étape, le pentest accroît l'efficacité et la performance du processus d'évaluation des risques.

Sur le plan de l'efficacité :

- Il donne l'occasion aux testeurs de se concentrer sur les risques les plus graves (la modélisation des menaces ayant probablement mis en évidence les menaces à faible risque).
- Il facilite l'atténuation des risques par le service informatique à un stade plus précoce du processus d'évaluation

Et sur le plan de la performance :

- Le pentest permet de valider les corrections déjà déployées.
- Il ajoute une couche de vérification supplémentaire qui peut repérer des vulnérabilités passées inaperçues

Posture de l'appareil et accès orienté identité (parcours « zero trust »)

Les technologies émergentes exigent des stratégies axées sur l'identité et une validation continue de la posture des appareils afin de protéger les données sensibles et de maintenir l'intégrité des opérations. Pour prendre en charge des parcs de plus en plus diversifiés, la gestion doit se moderniser en automatisant l'application des règles, en allégeant la charge des opérations et adoptant une approche « zero trust » à grande échelle.

Les solutions suivantes fournissent des outils à l'efficacité variable pour la gestion du cycle de vie des technologies émergentes :

- **Gestion des appareils mobiles (MDM)** : intègre la gestion des appareils, la gestion des identités et la sécurité des points de terminaison de façon exhaustive, **du déploiement sans intervention à l'élimination sécurisée**, sur site ou dans le cloud.
- **Gestion unifiée des points de terminaison (UEM)** : sur site ou dans le cloud, elle offre une prise en charge multiplateforme, mais son éventail de compétences est souvent plus restreint.
- **Amazon Web Services (AWS) :** modèle basé sur le cloud qui offre des fonctions de gestion et de sécurité limitées à des technologies spécifiques, comme les appareils IoT, et prend en charge plusieurs fournisseurs.
- **Gestion autonome des points de terminaison (AEM) :** l'avenir de l'UEM, basé sur le cloud ; elle réduit les coûts d'exploitation grâce à l'automatisation et implémente l'approche « zero trust« en validant et en corrigeant en permanence la posture des appareils, y compris dans les grands parcs mixtes.

Contrôle des applications et des données

Quels que soient le type d'appareil et l'OS qu'il utilise, les données sont des données. La protection des données reste au cœur de chaque contrôle, de chaque processus et de chaque tâche de la gestion et de la sécurité des technologies émergentes.

Pour sécuriser les appareils et les données qu'ils traitent et abritent, le déploiement de configurations s'avère particulièrement efficace. Les méthodes prises en charge dépendront largement de l'OS, mais l'objectif est d'établir des configurations sécurisées conformes aux bonnes pratiques, aux normes et aux cadres, afin de préserver la sécurité des données au-delà des frontières de l'OS.

Quelques exemples d'outils permettant de créer des configurations sécurisées :

- **Android** : **OEMConfig** et **Android Open Source Project** (AOSP)
- **Apple** : **Apple Configurator**, **Jamf Pro** et la **gestion déclarative des appareils** (DDM).
- **Linux** : scripts Bash, **SOTI MobiControl** et **Microsoft Intune**
- **Propriétaire :** consultez le site du fabricant pour obtenir des outils spécifiquement adaptés à la technologie.

Suivi et réponse

Une cybersécurité proactive repose avant tout sur une excellente visibilité de l'état de santé des points de terminaison. Plus les incidents sont identifiés rapidement, plus les mécanismes de réponse peuvent les atténuer de façon précoce. La surveillance active des points de terminaison de votre infrastructure n'est pas seulement fortement recommandée : c'est un élément crucial de l'architecture « zero trust ».

Celle-ci s'appuie sur des protections sur l'appareil et sur le réseau. Le réseau est abordé dans la section suivante ; voici d'abord quelques directives pour maintenir la posture des appareils dans toute votre infrastructure :

- Surveillez activement la télémétrie des appareils et leur niveau de conformité
- Intégrer vos solutions de gestion et de sécurité pour automatiser la réponse
- Mettez en œuvre le principe « zero trust » pour vérifier la santé des points de terminaison avant de leur accorder l'accès aux ressources
- Déployez régulièrement les correctifs de sécurité ainsi les mises à jour du système d'exploitation et des applications

Sécurité du réseau

Les technologies émergentes sont souvent plus performantes que les précédentes, ce qui complique la gestion de certains points de terminaison ou les rend incompatibles avec les objectifs de l'entreprise. Le risque reste une notion subjective, et il n'existe pas de stratégie de sécurité généraliste. D'où l'importance de sécuriser les données sur les points de terminaison eux-mêmes. Qu'elles soient déployées seules ou en combinaison, les solutions suivantes permettent d'optimiser la sécurité des données dans les environnements locaux et cloud :

- **Zones démilitarisées (DMZ)** : elles compartimentent les appareils à haut risque, IoT en tête, en n'autorisant qu'une communication contrôlée avec les systèmes internes ou les réseaux externes en fonction de règles strictes.
- **Réseau local virtuel (VLAN) :** il isole le trafic du réseau pour limiter les déplacements latéraux et appliquer le principe du moindre accès aux communications ; il offre au service informatique un contrôle fin sur la circulation des données entre les appareils et les systèmes essentiels à la mission de l'entreprise.
- **Orchestration, automatisation et réponse de sécurité (SOAR)** : cette solution unifie les outils et les workflows de sécurité grâce à l'automatisation pour accélérer la détection, la prise en charge et le confinement des menaces.
- **Accès réseau zero trust (ZTNA)** : procède à une vérification continue et contextuelle des appareils, met en place des microtunnels pour isoler chaque demande de connexion et effectue des contrôles de santé pour s'assurer que seuls les appareils conformes peuvent accéder aux ressources protégées.

Bases de référence, critères, normes et cadres

Il est important de considérer chaque section comme la phase d'un cycle plutôt que comme le segment d'une séquence linéaire. Dans les domaines de l'informatique et de la sécurité, les cycles de vie sont itératifs, ils ne sont pas une destination, mais un chemin sans fin, où chaque étape s'appuie sur la précédente pour informer la suivante. Dans cette optique, il faut une synergie parfaite entre les éléments suivants pour maintenir la sécurité malgré l'introduction de technologies émergentes dans votre environnement :

- **Profils de référence :** ensemble de contrôles et de processus qui **définissent une posture de sécurité fondamentale.**
- **Critères :** mesures de performance utilisées pour **évaluer la conformité aux bonnes pratiques de sécurité.**
- **Normes :** bonnes pratiques reconnues mondialement qui décrivent la manière dont le matériel, les logiciels et/ou les services doivent être **sécurisés pour répondre à une exigence spécifique**.
- **Cadres :** Directives structurées qui détaillent la façon dont les contrôles, les règles, les processus et **les normes doivent être déployés pour minimiser les risques** et maximiser la sécurité.

Conclusion

Armés d'une vision claire des technologies émergentes et de leur impact sur les objectifs de l'entreprise, les responsables d'activité et les équipes informatiques ont toutes les cartes en main pour passer à l'étape suivante : aligner les stratégies de gestion et de sécurité existantes sur des bonnes pratiques d'avenir. En agissant dès maintenant, les organisations vont garder une longueur d'avance sur les risques émergents, simplifier leurs opérations et aborder en toute confiance la prochaine vague d'innovation.

Check-list : Prochaines étapes pour les décideurs informatiques et métier

1. Identifiez les scénarios métier

- Identifiez les domaines où les technologies émergentes (IA, IoT, informatique spatiale, dispositifs corporels) font écho aux objectifs de l'entreprise.
- Déterminer leur ROI potentiel et les améliorations opérationnelles qu'elles peuvent apporter aux workflows existants.
- Donnez la priorité aux initiatives qui permettent d'obtenir des résultats concrets sur le plan de la performance commerciale ou de la conformité.

2. Mettez en place une équipe d'évaluation interfonctionnelle

- Formez un comité composé de spécialistes de l'informatique, de la sécurité, des affaires juridiques et des opérations.
- Répartissez les responsabilités de l'évaluation des risques, de l'examen de la conformité et de la gestion du cycle de vie.
- Définissez des canaux de communication pour accélérer les échanges d'information.

3. Réalisez un inventaire complet des actifs et des dépendances

- Documentez l'ensemble des appareils, logiciels, API et services cloud utilisés au sein de l'infrastructure.
- Identifiez les dépendances d'intégration dans les environnements hybrides (cloud, local et edge).
- Identifiez clairement les modèles de propriété (COBO/COPE/BYOD/CYOD) à des fins de visibilité et de transparence.

4. Procédez à des évaluations des risques et des menaces

- Utilisez des méthodes qualitatives et quantitatives pour évaluer la tolérance au risque et son impact.
- Cartographiez les menaces à l'aide de modèles dans un souci de précision et de cohérence.
- Classez les vulnérabilités en fonction de leur gravité, des possibilités d'exploitation et des délais de correction.

5. Réalisez des exercices de modélisation des menaces

- Simulez des trajectoires d'attaques potentielles à l'aide de cadres de modélisation des menaces reconnus.
- Identifiez les points d'exposition touchant la confidentialité, la circulation des données et les opérations.
- Documentez les mesures d'atténuation afin de réduire les risques avant la mise en production.

6. Validez les exigences en matière de conformité et de gouvernance

- Passez en revue les réglementations régionales et sectorielles.
- Clarifiez les questions de résidence et de souveraineté des données, ainsi que la gestion des risques liés aux fournisseurs tiers.
- Intégrez des considérations éthiques s'agissant de l'IA et des technologies basées sur les données.

7. Définissez des processus d'inscription et de provisionnement

- Normalisez les workflows d'intégration pour tous les types d'appareils et tous les modèles de propriété.
- Automatisez la configuration, la cadence des correctifs et les contrôles d'accès pour minimiser les erreurs manuelles.
- Utilisez l'inscription sécurisée et l'authentification basée sur l'identité pour vérifier les points de terminaison.

8. Intégrez les stratégies d'identité et d'accès

- Exigez une vérification constante des identifiants et de la posture de sécurité des appareils avant d'accorder l'accès aux ressources.
- Appliquez le principe du moindre privilège aux points de terminaison et aux applications.
- Intégrez le principe « zero trust » et des règles sensibles au contexte dans les systèmes de contrôle d'accès.

9. Mettez en place des configurations sécurisées et des contrôles des données

- Définissez des profils de sécurité de référence pour fixer les exigences de configuration et de conformité.
- Chiffrez les données sensibles au repos et en transit.
- Appliquez des règles granulaires pour la classification, le stockage et le partage des données.

10. Segmentez et durcissez les communications réseau

- Utilisez des VLAN et des DMZ pour isoler les appareils à haut risque tels que les appareils IoT et les dispositifs corporels.
- Appliquez la microsegmentation et l'accès réseau « zero trust » (ZTNA) pour mettre en œuvre des contrôles de sécurité flexibles sur le réseau.
- La sécurité des données est indissociable de celle du réseau, quels que soient le type et l'OS de l'appareil, le modèle de propriété et le lieu de travail.

11. Mettez en place des règles de surveillance continue et de réponse automatisée

- Collectez les données de télémétrie de tous les points de terminaison pour acquérir une visibilité en temps réel sur leur état de santé.
- Déployez des workflows automatisés pour détecter les anomalies et répondre aux incidents.
- Transmettez les alertes à un outil centralisé afin d'automatiser les tâches de détection et de correction des menaces.

12. Appliquez des profils de référence et des critères, et collectez des données de productivité

- Appliquez des normes de configuration de référence pour une sécurité homogène à l'échelle de l'entreprise.
- Utilisez des critères pour mesurer les performances et évaluer les postures de sécurité.
- Suivez les KPI pour évaluer le statut de conformité et chiffrer la réduction des risques.

13. Validez régulièrement votre stratégie à l'aide de tests de pénétration et d'audits

- Programmez des tests de pénétration récurrents et des analyses de vulnérabilité post-déploiement.
- Validez les corrections identifiées lors des exercices de modélisation des menaces.
- Contrôlez les résultats par rapport aux références établies et actualisez les règles en conséquence.

14. Automatisez la gestion du cycle de vie et l'application des règles

- Misez sur des systèmes de gestion unifiée ou autonome des points de terminaison pour une conformité constante.
- Automatisez l'application des correctifs, les règles de conformité et les workflows de mise hors service des appareils.
- Alignez continuellement les configurations sur l'évolution des cadres et des normes.

15. Documentez les résultats et organisez régulièrement des formations

- Créez des boucles de feedback pour consigner les enseignements face aux menaces émergentes.
- Misez sur la formation continue des administrateurs et des utilisateurs pour maximiser leur connaissance des risques.
- Réévaluez la pertinence des contrôles et adaptez-les à l'évolution des technologies et des réglementations.