jamf

Les failles de sécurité s'élargissent. Apprenez à les refermer.

Avec les pratiques de travail hybrides, les appareils mobiles et les menaces avancées, la sécurité du périmètre ne tient plus. Désormais, il faut adopter une approche multicouches.

LES RAISONS DE L'ÉCHEC DE SOLUTIONS TRADITIONNELLES

Le périmètre a disparu. Le risque est toujours là.

- La multiplication des appareils → élargit la surface d'attaque
- La mobilité → fait perdre du contrôle
- La complexité → ralentit la réponse

Les services cloud, le travail à distance, le BYOD et les réseaux non fiables ont érodé les frontières que les outils traditionnels étaient conçus pour protéger.

LE PAYSAGE DES MENACES

Les menaces actuelles sont sophistiquées, convergentes et implacables.

+ de 100 millions
d'enregistrements de clients ont été compromis lors de violations récentes

2,1 milliards
de téléchargements présentaient des vulnérabilités connues en 2023

25 M$
ont été perdus suite à une campagne de deepfake visant un directeur financier

+ de 90 %
des attaques exfiltrent désormais les données au lieu de les chiffrer

PRINCIPALES CATÉGORIES DE MENACES

Ingénierie sociale et hameçonnage

L'hameçonnage prend de nombreux visages : il utilise l'e-mail, les messageries vocales, les SMS et des codes QR, il cible des profils clés et exploite de nouvelles techniques telles que le faux mode avion et le faux mode Verrouillage.

Attaques d'États voyous et APT

90 % des alertes de sécurité proviennent de l'extérieur des infrastructures critiques Les principales cibles : l'éducation, les administrations et les groupes de réflexion. Le coût moyen : 1,6 million de dollars par incident

Attaques contre la chaîne d'approvisionnement

Elles ont triplé en 2023 et compromettent les partenaires et les fournisseurs pour obtenir des points d'entrée indirects

Menaces sur mobile

43 % des appareils compromis sont pleinement exploités (soit une augmentation de 187 % sur 12 mois). 80 % des sites d'hameçonnage ciblent les mobiles. Les logiciels malveillants uniques ciblant les mobiles ont augmenté de 51 %

Menaces renforcées par l'IA

D'après les observations, 5 groupes APT exploitent l'IA pour améliorer leurs capacités d'attaque

MENACES PROVENANT D'ÉTATS VOYOUS

Les attaques ciblées en chiffres.

Principaux secteurs ciblés

- Éducation 100 %
- Administration 75 %
- Groupes de réflexion/ONG 69 %
- Informatique 69 %

9 sur 10
le nombre d'organisations qui pensent avoir été ciblées par des acteurs malveillants affiliés à des États.

1,6 M$
le coût moyen d'un incident provoqué par un État-nation

IL N'Y A PAS DE SOLUTION GÉNÉRIQUE

Le paysage des appareils a changé.

Les solutions traditionnelles conçues pour les ordinateurs de bureau fixes ne peuvent pas sécuriser les environnements dynamiques et la diversité des appareils d'aujourd'hui.

25%
Part de marché de macOS aux États-Unis

96%
des RSSI prévoient une croissance du parc de Mac dans les 12 à 24 prochains mois

3,6 %
Nombre moyen d'appareils par utilisateur dans le monde (2023)

96%
Des appareils mobiles présents sur les réseaux d'entreprise sont des appareils personnels

LES APPAREILS MOBILES : UN RISQUE NON MAÎTRISÉ

Les appareils mobiles sont une véritable porte d'entrée que personne ne garde.

L'utilisateur moyen possède 3,6 appareils. Ce sont autant de vecteurs d'attaque par personne, et ils sont rarement équipés de solutions spécialisées de protection des points de terminaison.

43%
Des appareils compromis sont entièrement exploités (augmentation de 187 % sur 12 mois)

80%
Des sites d'hameçonnage ciblent les appareils mobiles

51%
Augmentation du nombre de logiciels malveillants uniques ciblant les mobiles (plus de 920 000 échantillons)

96%
Des appareils mobiles présents sur les réseaux d'entreprise sont des appareils personnels

CADRE STRATÉGIQUE

Les quatre C pour combler les lacunes de sécurité.

1. **Cohérence**
Traitez chaque point d'extrémité de la même manière, quel que soit le type d'appareil, son format, son système d'exploitation ou son modèle de propriété.

2. **Conformité**
Établissez des profils de référence, surveillez les anomalies et conservez des preuves vérifiables grâce aux données de télémétrie.

3. **Consolidation**
Réunissez les équipes informatique et de sécurité pour briser les silos, partager les informations et unifier les flux de travail.

4. **Économies de coûts**
Maximisez la rentabilité de vos investissements en misant sur des outils natifs, l'automatisation, des processus rationalisés et des programmes de BYOD.

MODÈLE DE SÉCURITÉ MULTICOUCHE

Défense en profondeur = chaque couche détecte ce que les autres ne voient pas.

Si une menace parvient à contourner un contrôle, la couche suivante est là pour l'arrêter. L'intégration de ces trois fondamentaux crée des mesures palliatives dans l'ensemble de votre infrastructure.

Gestion des appareils
Déployez des configurations, appliquez les règles et gardez le contrôle à grande échelle.

Gestion des identités
Vérifiez les utilisateurs et les appareils avant de leur accorder l'accès aux ressources protégées.

Sécurité des points de terminaison
Détectez et répondez aux menaces sur tous les appareils en temps réel.

Gestion + Identité + Sécurité → Défense en profondeur

TECHNOLOGIES CLÉS

Comment les couches fonctionnent en pratique.

Déploiement sans intervention
Des appareils sécurisés dès la première mise sous tension. Les configurations, les applications et les règles sont déployées automatiquement lors de l'installation des appareils d'entreprise et BYOD.

Recherche des menaces
Les menaces inconnues sont détectées de façon proactive grâce aux profils de référence, à la télémétrie et aux workflows de remédiation automatisés.

ZTNA
Ne jamais faire confiance, vérifier systématiquement. Les VPN traditionnels sont abandonnés au profit de microtunnels chiffrés, du principe de moindre privilège et de contrôles d'intégrité continus.

Réponse aux menaces avancées
Analyse des IoC et des IoA, reconstitution de la chronologie et élimination des APT. Les délais d'enquête passent plusieurs semaines à quelques minutes seulement

RÉSULTATS

Pourquoi c'est une mesure essentielle.

Une protection renforcée sur tous les appareils

Une détection des menaces plus rapide pour une réponse immédiate

Une charge opérationnelle réduite

Une sécurité cohérente dans tous les environnements

Découvrez le cadre complet permettant de mettre en place une sécurité multicouches intégrée au sein de votre organisation.

jamf

Téléchargez le livre blanc

www.jamf.com/fr/