digitim
MODERN WORKPLACE SERVICES

LIVRE BLANC - MAI 2025

CYBERSÉCURITÉ 2025
PROTÉGER SON ENTREPRISE À L'HEURE DES MENACES MOBILES

Une approche concrète pour accompagner les DSI dans la défense active de leur système d'information, grâce à des outils adaptés et des services managés sur-mesure.

SOMMAIRE

POURQUOI CE LIVRE BLANC ?

En 2025, la menace cyber ne faiblit pas. Pire : elle se transforme, se perfectionne, se déplace vers des terminaux autrefois jugés secondaires. Avec l'essor du travail hybride, des outils SaaS, des usages mobiles et d'une IT de plus en plus distribuée, le smartphone est devenu l'un des maillons faibles du système d'information.

Ce livre blanc s'adresse aux DSI, aux responsables de la sécurité informatique, aux acheteurs IT, aux élus et gestionnaires de parc informatique dans le public comme dans le privé. Il ne promet pas des solutions miracles. Il propose des réponses concrètes, activables, et une méthodologie précise pour reprendre le contrôle.

Avec ses partenaires, notamment LOOKOUT, et ses solutions internes comme l'outil DEX (Digital Employee Experience) QUANTOOM, DIGITIM accompagne déjà des dizaines d'entreprises et de collectivités dans la maîtrise de leur cybersécurité mobile.

2. ÉTAT DES LIEUX : UNE MENACE INVISIBLE MAIS BIEN PRÉSENTE

Selon le rapport Lookout 2024 :

- **33 % des organisations ont enregistré au moins une application malveillante installée sur un terminal professionnel mobile.**
- **Les attaques de phishing par SMS (smishing) ont augmenté de 30 % en un an.**
- **52 % des entreprises victimes d'attaques mobiles n'avaient aucun système de surveillance de leurs terminaux.**

EXPLOSION DES MENACES ET DES COÛTS

- En 2024, le coût annuel des cyberattaques en France a dépassé **les 100 milliards d'euros**, un record qui souligne l'ampleur du phénomène et son impact économique direct sur le tissu entrepreneurial français.
- Le marché français de la cybersécurité, pour répondre à cette menace croissante, devrait **passer de 4 milliards d'euros en 2023 à plus de 6,2 milliards d'euros en 2028**, soit une hausse de plus de 50 %.

PRÉVALENCE DES ATTAQUES

- **43 % des organisations françaises ont subi au moins une cyberattaque réussie en 2024**, représentant 385 000 incidents recensés, soit plus de 1 000 attaques par jour.
- Près de **49 % des entreprises déclarent avoir été victimes d'une cyberattaque en 2023**, et la tendance est à la hausse pour 2025.
- **73 % des entreprises touchées citent le phishing comme mode d'attaque principal**, suivi par l'exploitation de failles (53 %) et l'arnaque au président (38 %).

ÉVOLUTION ET SOPHISTICATION DES MENACES

- **Le volume des cyberattaques a augmenté de 140 % entre 2020 et 2024**, porté par la généralisation de l'intelligence artificielle et la multiplication des objets connectés, ce qui rend les attaques plus difficiles à détecter et à contrer.
- Les compromissions de sites, messageries ou applications sont **en hausse de 25 % par rapport à 2023**.

FACTEURS HUMAINS ET ORGANISATIONNELS

- **46 % des failles de sécurité sont dues à des erreurs humaines**, ce qui souligne l'importance de la formation et de la sensibilisation continue des collaborateurs.
- **Deux entreprises sur trois ne disposent pas de solution de protection** pour leurs applications web, ce qui constitue un point d'entrée majeur pour les cybercriminels.

Les appareils mobiles (smartphones, tablettes) sont souvent moins bien sécurisés que les postes fixes :

- pas ou peu de MDM installé,
- utilisateurs mêlant usages pro et perso,
- réseaux Wi-Fi publics utilisés,
- accès aux données sensibles via des apps non contrôlées.

3. QUELLES CONSÉQUENCES POUR VOTRE ORGANISATION ?

Lorsqu'un terminal est compromis, c'est l'ensemble de la chaîne de sécurité qui est exposée.

Une mauvaise sécurisation des informations peut avoir des conséquences dramatiques :

Les coûts indirects d'une cyberattaque mobile sont élevés :

- mobilisation des équipes,
- perte de productivité,
- incident de communication,
- redéploiement technique...

Les impacts des défaillances en cybersécurité pour les entreprises

- **Perte ou vol de données** (clients, stratégie, RH)
- **Infection du réseau interne par propagation**
- **Demande de rançon** (ransomware)
- **Altération de l'image de l'entreprise**
- **Risques juridiques** (RGPD, conformité DORA, etc.)
- **Perte financière :** Le coût moyen d'une cyberattaque pour une entreprise atteint 4 millions d'euros.
- **Ralentissement des opérations :** Arrêt des systèmes d'information, perte de productivité.
- **Pertes de données :** Confidentialité compromise et risque juridique.
- **Réputation endommagée** : La confiance des clients et partenaires est mise en péril.

LES SECTEURS A HAUT RISQUE

Certains secteurs sont particulièrement vulnérables aux cyberattaques :

- **Avocats et conseillers juridiques :** Vol de données confidentielles via des e-mails non sécurisés.
- **Transactions M&A :** Échange d'informations financières critiques entre plusieurs intervenants.
- **Industrie pharmaceutique :** Exposition des brevets et de la propriété intellectuelle.
- **Conseils d'administration :** Risque d'échange de documents sensibles via des solutions non sécurisées.

4. SOLUTIONS ET BONNES PRATIQUES POUR RENFORCER LA SÉCURITÉ DES DONNÉES

LES RISQUES HUMAINS ET COMMENT Y REMÉDIER

Les erreurs humaines sont souvent le maillon faible. Pour y répondre :

- **Sensibilisation et formation continue :** DIGITIM propose des programmes de prévention pour limiter les risques.
- **Authentification renforcée :** Utilisation de solutions comme le MDM pour sécuriser les accès aux terminaux.
- **Politique d'accès aux données :** Restreindre l'accès selon les rôles et besoins des collaborateurs.

DES SOLUTIONS TECHNIQUES PERFORMANTES

Pour protéger les dispositifs et les informations :

A) QUANTOOM : UN PORTAIL IT POUR FACILITER LES USAGES IT ET APPLIQUER LES PROCEDURES

- Suivi temps réel des appareils
- Alertes de non-conformité ou de comportement à risque
- Connexion aux outils SIRH pour gérer onboarding/offboarding
- Suivi des coûts, des usages et de l'empreinte carbone

B) UN MDM ADAPTE A VOS PARCS : JAMF (APPLE), INTUNE (MICROSOFT), IVANTI, WORKSPACE 1...

- **Supervision via MDM :** DIGITIM déploie des solutions de **Mobile Device Management** pour gérer, sécuriser et suivre les terminaux mobiles de votre flotte.
- Déploiement distant, sécurisation des apps et données
- Gestion de flottes hétérogènes
- Applications métier et contrôle des accès (Zero Trust possible)
- **Effacement à distance :** En cas de perte ou de vol, effacer instantanément les données sur les appareils mobiles.

C) UNE STRATEGIE D'INFOGERANCE

- Externalisation du run et du support utilisateurs
- Mise en place de helpdesk et tickets
- Maintenance, garantie, réattribution

D) PROTECTION PROACTIVE AVEC LOOKOUT MOBILE ENDPOINT SECURITY

- Analyse comportementale des apps
- Détection de phishing, malwares, failles Zero-day
- Interruption automatique des connexions malveillantes
- **Audits réguliers :** Évaluation des vulnérabilités pour anticiper les failles de sécurité.

LA PROTECTION JURIDIQUE

Respecter la réglementation européenne avec des prestataires comme DIGITIM, qui garantissent :

- **Des serveurs sécurisés en Europe** conformes au RGPD.
- **Une traçabilité complète** des données grâce à des solutions certifiées.

LA CYBERSECURITE, UN INVESTISSEMENT STRATEGIQUE

Dans un monde ultra-connecté, la cybersécurité est un **investissement indispensable** pour assurer la pérennité de votre entreprise. DIGITIM, acteur engagé dans la sécurisation des flottes mobiles, offre des solutions complètes pour :

- Protéger vos terminaux et vos données avec des outils de pointe.
- Sensibiliser vos équipes pour minimiser les risques humains.
- Assurer la conformité et la tranquillité de votre organisation.

> **Protégez votre entreprise dès maintenant avec DIGITIM et nos partenaires spécialisés.**
>
> **Contactez nos experts pour une étude personnalisée et sécurisez vos dispositifs avec des solutions innovantes.**

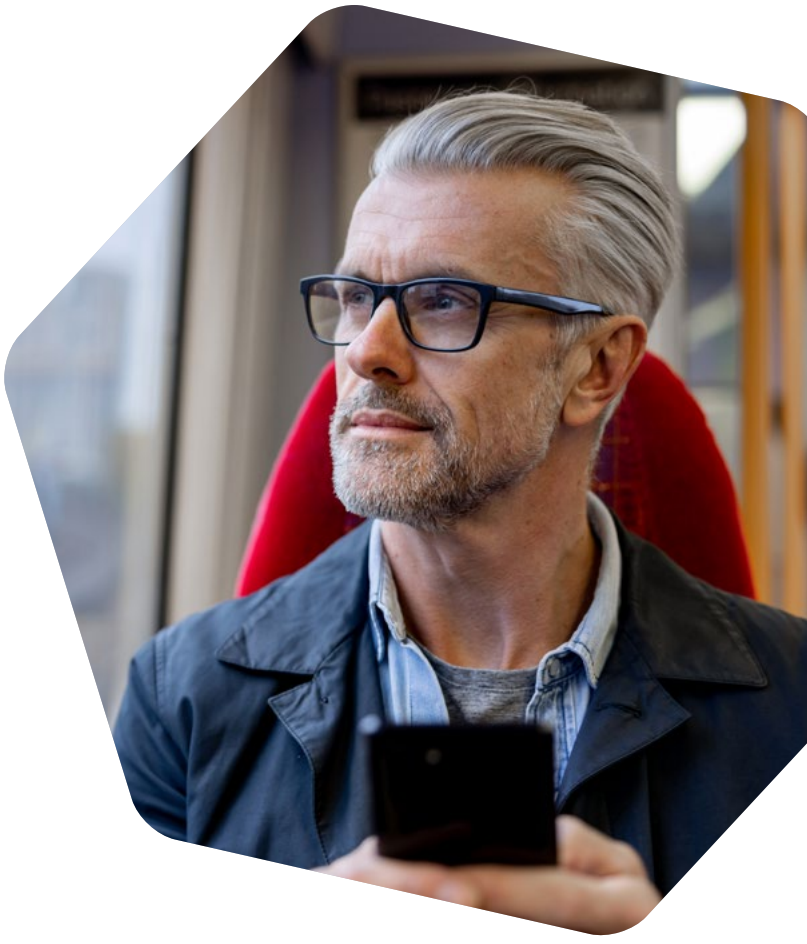
5. BONNES PRATIQUES : LES RÉFLEXES À ADOPTER DÈS AUJOURD'HUI

POUR VOS COLLABORATEURS :

- Former sur les risques mobiles (SMS suspects, apps inconnues...)
- Renforcer les mots de passe (ou opter pour une solution SSO + MFA)
- Éviter les connexions à des réseaux publics

POUR VOTRE DSI :

- Réaliser un audit des devices en circulation (pro/perso)
- Activer un MDM si ce n'est pas encore fait
- Mettre en place un plan d'escalade en cas d'incident



6. ET DEMAIN ? L'IA AU SERVICE DE LA CYBERSÉCURITÉ

Les solutions partenaires comme Lookout ou les fonctions prédictives de Quantoom permettent aujourd'hui :

- D'anticiper les failles
- De prévoir les pannes ou incidents matériels
- D'automatiser les actions correctives avant qu'il ne soit trop tard

UN SYSTEME DE DEFENSE MOBILE A 360°

La cybersécurité mobile ne peut plus être traitée comme un sujet annexe. Avec l'accélération des usages hybrides, c'est un pilier central de votre gouvernance IT.

DIGITIM vous accompagne avec des outils puissants (QUANTOOM), des solutions tierces de pointe (LOOKOUT), et un support humain, pédagogique, accessible.

Pour aller plus loin, vous pouvez lire nos articles sur :

- Le Mobile Device Manager : un levier stratégique pour les DSI
- La Digital Employee Experience (DEX) notre outil Quantoom

Pour garantir une experience numérique des collaborateurs optimales, la sécurité est incontournable.

Vous voulez passer à l'action ?

- **Demandez un audit cybersécurité de vos actifs mobiles.**
- **Testez gratuitement Quantoom pendant 30 jours.**

Un seul contact ! hello@digitim.fr

Rédigé par l'équipe **Digitim**, en partenariat avec **Lookout**.

Mise à jour avril 2025


digitim
MODERN WORKPLACE SERVICES