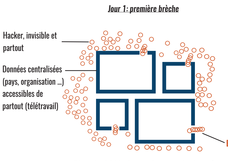
Protégez l'avenir de votre entreprise

Renforcez votre résilience face aux cyber-attaques et rançongiciels

Problème #1 : La centralisation des accès (Single Sign-On, mot de passe maitre) est le talon d'Achille des entreprises

Il suffit de14 jours entre une première intrusion et un raid sur tout le réseau



Plus de 80% des violations de données commencent par l'utilisation d'un mot de passe faible, volé ou réutilisé

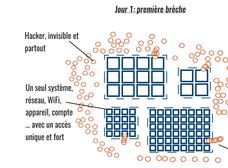
Remède #1 : Séparer l'accès à chaque système et décentraliser les identifiants

Principe: Tout comme pour le COVID-19, arrêter la propagation d' un virus nécessite une «distanciation sociale».

Comment faire? Séparez les accès de chaque système, réseau, WiFi, application, compte, appareil... et décentralisez les identifiants d'accès pour que si l' un d'eux est volé, les autres restent en sécurité.

Résultat : Pas de point d'accès centralisé ni de mot de passe principal

Les brèches de données sont confinées par défaut



Clusters de données plus petits, accès indépendants, pas de mouvement latéral

Problème #2 : Le cerveau humain ne peut pas retenir de mots de passe forts

Forteresse MyCena
(brevet en instance)
Trois niveaux de sécurité (Bronze, Argent, Or) pour des mots de passe de différentes sensibilités

Remède #2 : Protégez vos mots de passe dans une forteresse locale à laquelle vous seul avez accès

Principe: Vous n'avez pas besoin de vous souvenir des mots de passe. Il vous suffit d' être le seul à pouvoir y accéder et les utiliser.

Comment faire? Utilisez MyCena, une solution décentralisée qui remplace le cerveau dans la gestion de mots de passe uniques et forts.

MyCena crée des mots de passe uniques et forts pour chaque système, appareil, réseau, application ... et les protège dans une forteresse locale d'identifiants à laquelle vous seul avez accès.

Plus besoin de créer, mémoriser, taper ou voir un seul mot de passe!

Et surtout, il n' y a pas de mot de passe maitre, ni de point d'accès centralisé, donc vous ne risquez donc pas de tout perdre en cas de brèche.

Résultat : Mots de passe uniques et forts pour chaque système utilisé

Réduisez le risque de perte totale de données, de rançongiciel et de perturbation des activités

Portefeuille de solutions MyCena

Solution	MyCena Personal Fortress (MPF)	MyCena Business Fortress (MBF)	MyCena Desk Center (MDC)
Usage	Individuel	Entreprise (avec console)	Entreprise (avec console)
Support	Integration Mobile + Bureau	Integration Mobile + Bureau	Bureau (pour environnements containeurisés)
Idéal pour	Usage personnel	Business, télétravail	Centres de contact, centres d' appels, BPO et BPS

Simplifiez la gestion des informations d'identification forts et uniques

avec la console MyCena

Console MyCena

POUR MYCENA BUSINESS FORTRESS ET MYCENA DESK CENTER

- Gérer les mots de passe, les politiques de mot de passe des systèmes et les attributs
- Gérer les rôles et permissions (MDC uniquement)
- Gérer la liste des utilisateurs (télécharger la liste ou utiliser Active Directory)
- Gérer qui reçoit quelles informations d' identification (gérer les attributs)
- Surveiller l' utilisation et les fraudes potentielles (module complémentaire: Gouvernance, Risque et Conformité)

Authentification Sécurisée Simplifiée (3SO)

Pour tous les utilisateurs

MyCena Desk Center pour ordinateurs (Mac, Windows ou Linux)

GESTION DES INFORMATIONS D'IDENTIFICATION POUR LES LIEUX DE TRAVAIL CONFINÉS

- Centres de contact, centres d' appels et BPO
- Organisations dont les employés traitent des informations très sensibles (Informations personnelles identifiables, informations financières, propriété intellectuelle ...) avec des risques élevés de fraudes / fuites
- Organisations dont les employés doivent accéder à plusieurs systèmes, réseaux, applications, comptes et bases de données pour un ou plusieurs clients

MyCena Business Fortress pour les appareils mobiles (iOS ou Android)

GESTION DES INFORMATIONS D'IDENTIFICATION POUR LES FORCES DE TRAVAIL DECENTRALISÉES

- Organisations qui ont déplacé leurs données vers le cloud, rendant les données accessibles de n' importe où
- Organisations dont les employés travaillent à domicile (WFH), ce qui augmente la surface des attaques pour le phishing, l' ingénierie sociale et les attaques par force brute
- Organisations utilisant Active Directory, créant de gros clusters de données pour les pirates
- Organisations utilisant l' authentification unique ou une identité centralisée, points d' entrée idéaux pour les pirates

Les avantages de MyCena

Pour l'organisation

Gérer des mots de passe uniques et forts

- ✓ **Distribuez des mots de passe forts et uniques pour chaque système, réseau, compte, base de données, WiFi ...**
- ✓ Gérez les politiques de mot de passe et surveillez leur utilisation sans voir les mots de passe des utilisateurs.
- ✓ Plus de mot de passe principal, d' identifiant unifié ou de point de défaillance central ni pour l' utilisateur, ni pour l' entreprise
- ✓ Déployez rapidement sans modernisation du système ni changement de l' infrastructure existente.
- ✓ Économisez 50% de vos coûts d'appels en support informatique liés à la réinitialisation de mots de passe
- ✓ Être conforme au RGPD (UE), CCPA (Californie), LGPD (Brésil), NYPA (NY), HIPAA, PCI DSSÊtre conforme au

Pour les utilisateurs

Authentification sécurisée simplifiée (3SO)

- ✓ Meilleure productivité: **Aucun mot de passe à créer, saisir, voir ou mémoriser**
- ✓ Meilleure sécurité: les mots de passe cryptés sont uniquement accessibles par le propriétaire avec une combinaison d' empreinte digitale, d' identification faciale, de code PIN, de schéma de verrouillage et de phrase vocale
- ✓ Meilleure protection: trois niveaux de sécurité (bronze, argent ou or) pour des mots de passe de sensibilités différentes

info@mycena.co
www.mycena.co