Evidian

Nomadisme : fédérer et protéger les accès Web

Trusted partner for your **Digital Journey**

Sommaire

Augmenter l'efficacité des utilisateurs nomades grâce aux accès Web

L'accès des utilisateurs nomades aux applications où qu'elles soient est un besoin vital pour l'activité de l'entreprise. Les fusions, acquisitions, délocalisations, le télétravail et le besoin d'accéder à l'information en temps réel sont une nécessité pour maintenir et augmenter la compétitivité de l'entreprise.

Les utilisateurs nomades peuvent être des conseillers commerciaux, des distributeurs, des fournisseurs, des partenaires... ayant besoin entre autre :

- d'accéder au système de relation client (CRM) en mode Saas ;
- de passer des commandes via un système de prise de commande unique hébergé dans un Cloud privé ;
- de suivre la situation des encours du client sur le système informatique interne ;
- de connaître l'état des stocks via des applications exploitées dans un data center de l'entreprise ;
- d'assurer la maintenance d'une infrastructure géographiquement répartie.

Si ces personnes accèdent en ligne facilement et en toute sécurité aux applications, les processus de l'entreprise s'en trouveront fortement optimisés.

Ce livre blanc décrit le cas d'un de nos clients opérateur de télécommunication qui, en optimisant les processus internes, gère la croissance de la demande tout en dégageant une marge de plus en plus importante :

- en offrant à ses conseillers une interface unique pour accéder à l'ensemble des informations et des encours d'un client, aux stocks... afin de lui permettre de mieux cerner le client et de lui proposer de nouveaux produits ou services ;
- en informant à tout moment les techniciens ou sous-traitants, via des alertes et consignes pour la réparation et le suivi des éléments défaillants de son infrastructure. Ceci afin de garantir le meilleur niveau de qualité de service tout en optimisant les coûts associés.

Il propose une réponse pragmatique aux questions suivantes :

- comment offrir rapidement, à un conseiller en agence ou technicien en intervention, un accès Web avec le niveau de sécurité adapté à leurs missions respectives ?
- comment fédérer et sécuriser les accès Web sans modifier les applications existantes (internes ou externalisées) : Cloud Privé, Saas ou hébergées ?
- comment éviter que les utilisateurs ne stockent leurs mots de passe applicatifs sur des environnements professionnels ou personnels (postes de travail, tablettes, smartphones, et terminaux mobiles) et introduisent ainsi des vulnérabilités ?

La suite de ce document décrit les besoins et la solution répondant à ces enjeux et ne nécessitant aucun composant client et aucune particularité sur le terminal mobile.

Mettre en place de nouveaux services par un portail « Corporate »

Conseil auprès de la clientèle et vente de nouveaux services

Notre opérateur de télécommunications a décidé de mettre en place un nouveau service commercial global pour la prise de commande unique de toutes ses offres. Grâce à une vue globale des informations de son client, le conseiller peut établir très rapidement des propositions complémentaires, qu'il soit situé en agence ou chez des partenaires distributeurs de ses offres.

L'objectif de ce nouveau service est de bénéficier des informations relatives à son client (produits et services déjà souscrits) pour lui proposer en temps réel des offres adaptées.

Un service qui couvre l'ensemble des opérations de vente

Ce nouveau service doit accélérer l'ensemble des processus opérationnels liés aux actions de vente en agence.

- le département commercial consulte et gère les informations clients et les contrats souscrits, au travers de l'application CRM Salesforce accessible via le web dans le Cloud Privé ou en mode Saas ;
- le département en charge des contrats Mobile donne accès aux conditions de vente des forfaits, souscription, pack mobile et système de prise de commande via une application Web hébergée dans un data center privé. Les autres départements font de même afin de proposer une offre Multiplay ;
- les conseillers, internes en agence ou externes chez les distributeurs, peuvent mettre à jour via le Web le système de prise de commande unique au moment de la vente.

Les opérations effectuées, après une authentification réussie, sont ainsi parfaitement identifiables « qui - où - quand », traçables et auditables par la compagnie qui souhaite les contrôler.

Maintenance d'une infrastructure géographiquement répartie

Notre opérateur de télécommunications a décidé de mettre en place un service global de suivi et de distribution du matériel nécessaire aux opérations de maintenance de son infrastructure.

L'objectif de ce nouveau service sécurisé est de gérer et d'affecter de façon fiable et rapide les matériels en réserve chez ses prestataires afin d'accélérer les interventions.

Un service qui couvre l'ensemble des opérations de maintenance

Ce nouveau service doit accélérer l'ensemble des processus opérationnels liés aux opérations de maintenance.

- le département de suivi des mouvements matériels peut gérer, au travers de l'application Web, la demande d'intervention du prestataire le plus approprié en fonction de la disponibilité du matériel et des attributs des contrats ;
- les équipes d'intervention, prestataires internes ou externes, peuvent mettre à jour via le Web la liste des matériels disponibles ou obtenir les informations qu'elles désirent sur leurs dossiers personnels ;
- la compagnie a la possibilité de suivre et de contrôler les opérations effectuées.

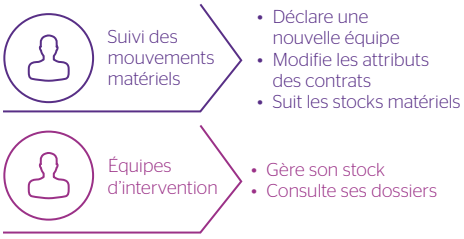
Des gains opérationnels immédiats

Ce nouveau service permet d'optimiser les processus liés à l'organisation des ventes et des interventions, ainsi qu'à la réalisation des opérations elles-mêmes.

L'accès direct aux applications Web en toute sécurité par les agences, les distributeurs et les agents de la compagnie, accélère et améliore la productivité commerciale ainsi que la gestion des opérations d'intervention.

La gestion de la prise de commande directement via le Web, par les conseillers en agences ou chez les distributeurs, avec accès direct à l'ensemble des informations du client, augmente l'efficacité commerciale des conseillers.

La déclaration et le suivi des mouvements des matériels effectués directement via le Web par les différents intervenants diminuent le coût de gestion des interventions et accélèrent la prise de décision.



Risques potentiels détectés pour la mise en place d'un tel service

Si le service génère des gains immédiats, il peut introduire des risques qui doivent être maîtrisés.

Les données manipulées par les conseillers commerciaux et les équipes d'intervention dans le cadre de ce nouveau service sont au coeur de la qualité de service de l'opérateur. Un contrat dont les données sont mal renseignées, une offre promotionnelle appliquée indûment, une opération de remboursement non justifiée, un état du stock non mis à jour peut avoir des répercutions très importantes sur le chiffre d'affaire, les délais d'intervention et la qualité de service, c'est-à-dire le business et donc le revenu.

De plus, certains utilisateurs, comme les distributeurs, accèdent à ce nouveau service à partir d'Internet et de terminaux non gérés par la compagnie, c'est-à-dire en dehors de la zone intranet protégée du Système d'Information.

- l'opérateur ne maîtrise pas la politique de sécurisation des postes de travail des prestataires externes ni du navigateur utilisé ;
- sans protection du portail, les prestataires externes pourraient accéder à toutes les applications de la compagnie via Internet ;
- l'opérateur souhaite utiliser les services en Saas, dans le Cloud et chez un hébergeur. Il doit absolument conserver la maîtrise des utilisateurs habilités à se connecter à ses applications Web.

La protection des données et leur accès via le Web ont rapidement été identifiés comme des points à maîtriser pour le succès de ce nouveau service.

Cas d'usage : solution mise en place par un opérateur télécom

Protéger et gérer les accès

Pour protéger les données, cet opérateur a mis en oeuvre un point de contrôle d'accès Web sécurisé intégrant 3 fonctions :

- filtrage réseau par pare-feu ;
- contrôle des accès utilisateurs avec mise en oeuvre d'une solution d'authentification et d'autorisation des accès ;
- Single Sign-on (authentification unique) sur les applications Web autorisées.

Les fonctions de contrôle des accès et de Web SSO sont effectuées par le logiciel Web Access Manager (WAM).

Web Access Manager, votre infrastructure de sécurité pour le Web

Web Access Manager (WAM) est une solution de sécurité qui authentifie les utilisateurs puis contrôle pour chaque requête HTML les droits d'accès aux URL demandées.

Contrôle centralisé des accès

Pour chaque URL demandée par un utilisateur, Web Access Manager vérifie les droits d'accès de l'utilisateur et autorise ou bloque, si nécessaire, la requête.

Web Access Manager est positionné à l'entrée de la zone la plus protégée du système d'information. C'est ainsi un point de passage obligé pour atteindre les applications. Tous les accès aux applications sont filtrés.Les fonctions de contrôle des accès et de Web SSO sont effectuées par le logiciel Web Access Manager (WAM).

Garantir la confidentialité des accès

La compagnie a souhaité mettre en oeuvre une communication SSL. Cette communication HTTPS s'effectue au niveau de Web Access Manager. Puisque seul ce serveur frontal est accessible de la toile, les serveurs Web applicatifs ne nécessitent pas de mise en oeuvre du SSL ; il n'y a pas de gestion de certificats supplémentaires.

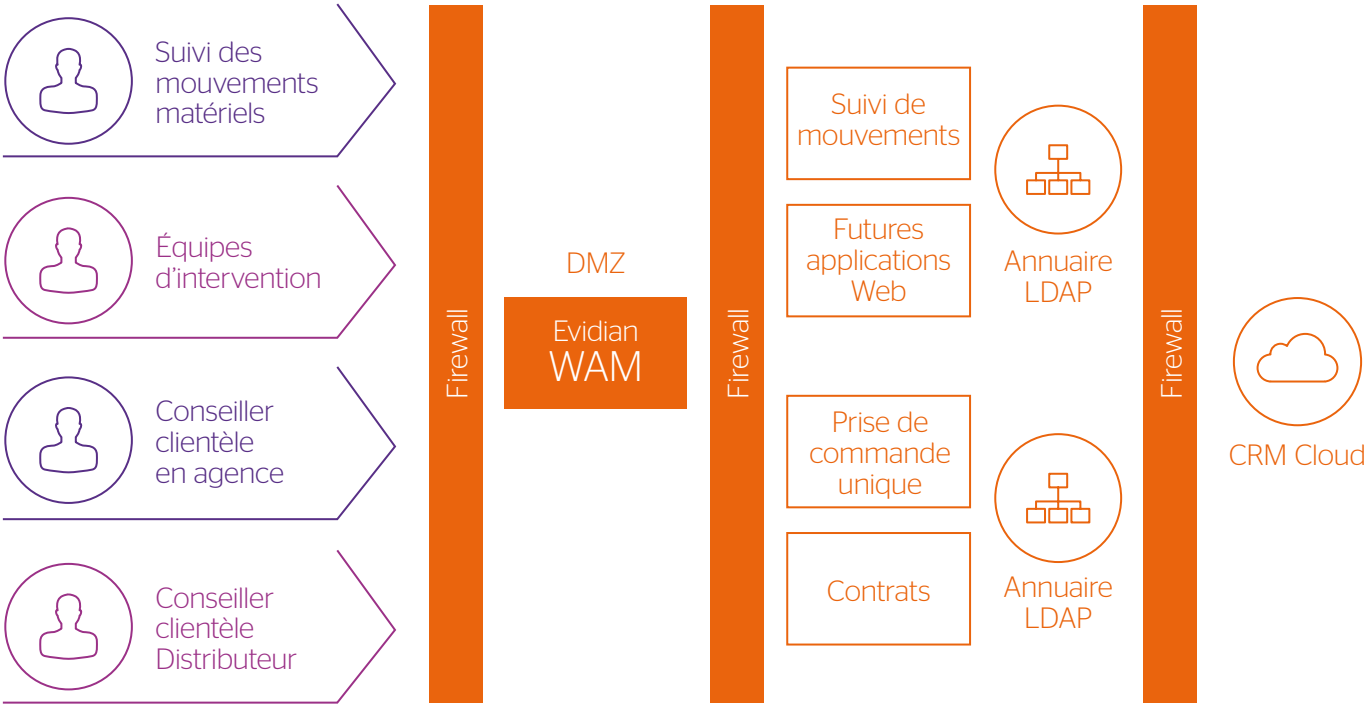
Simplifier les accès avec un Web SSO et une page d'accueil personnalisée

Web Access Manager simplifie les accès grâce à :

- une authentification primaire lors de la connexion de l'utilisateur ;
- une page d'accueil personnalisée qui présente les seules applications autorisées ;
- un accès automatique aux applications avec réauthentification secondaire transparente auprès de l'application. Cette fonction est aussi appelée Single Sign-On (SSO).

Web Access Manager accélère le déploiement de nouveaux services business Web

L'architecture de Web Access Manager a été un facteur clef dans le déploiement sécurisé de nouvelles applications Web.



Fonctions Web Access Manager	Mise en oeuvre de nouveaux services business Web
Intégration avec le répertoire LDAP de l'opérateur	Accélère la création d'accès Web en ligne 24x7
Authentification forte, SSO et contrôle d'URL et de l'adresse IP de l'utilisateur	Garantit la sécurité et la confidentialité de l'information
Architecture Reverse Proxy non intrusive (aucun module sur les serveurs Web applicatifs)	Isole les fonctions de sécurité des applications Web Pas de modification des applications
Administration centralisée	Simplifie l'ajout de nouveaux serveurs et applications Web
Console Web Access Manager	Permet de bloquer en quelques clics les accès d'un utilisateur
Audit centralisé	Analyse les activités des utilisateurs

La déclaration de l'application Web de suivi des mouvements de matériels dans Web Access Manager s'est effectuée en moins d'une heure (tests compris).

De même, une nouvelle application (d'éligibilité au dégroupage des lignes Télécom) a été déclarée en quelques dizaines de minutes dans le serveur Web Access Manager. Ceci sans modifier aucune application.*

*Informations non contractuelles

Contrôler et sécuriser l'accès utilisateur avec Web Access Manager

Généralement, quand les entreprises évoluent vers l'accès en ligne, il incombe aux administrateurs de chaque application de mettre en oeuvre la sécurité. Avec la multiplication des applications, les règles de sécurité deviennent rapidement impossibles à gérer. Ce type d'approche « puzzle » de la sécurité aboutit à des problèmes de sécurité et à la frustration de l'utilisateur final.

Mettre en place le contrôle d'accès à toutes les applications

Web Access Manager permet de définir et de gérer les applications et les ressources auxquelles peuvent accéder les utilisateurs. Afin d'éviter que chaque administrateur de ressources ne contrôle la sécurité sur ses serveurs, Web Access Manager centralise la gestion du contrôle d'accès aux ressources Web.

A l'aide d'une console facile à utiliser, un administrateur peut contrôler l'accès des utilisateurs de façon dynamique. Les nouveaux employés peuvent être ajoutés aux groupes appropriés et avoir immédiatement accès aux diverses applications. Avec Web Access Manager, il suffit d'un clic pour interdire l'accès aux services de l'entreprise aux anciens employés et partenaires. En outre, Web Access Manager permet de suivre l'activité de tous les utilisateurs. Avec Web Access Manager Web, vous pouvez mettre en oeuvre une politique de sécurité complète pour l'ensemble des ressources Web, internes et externes.

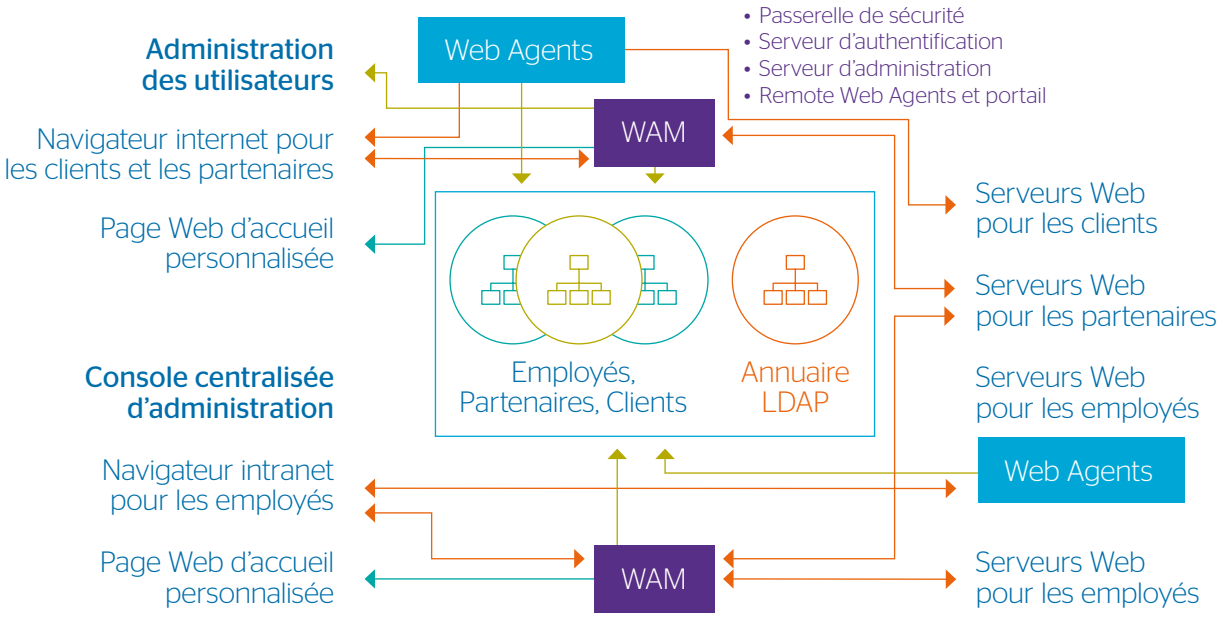
Contrôler les accès aux applications et aux URL

Les modules de contrôle des accès aux URL de Web Access Manager peuvent être positionnés, soit sur une passerelle de sécurité qui vient en rupture de flux, soit auprès des applications elles-mêmes sur les mêmes serveurs.

Web Access Manager permet de mettre en place quatre types d'architecture :

- purement « portail » dans laquelle le contrôle des accès se positionne en rupture de flux sur un point de passage obligé unique. Cette architecture est privilégiée car elle n'a aucun impact sur les applications et les serveurs d'applications ;
- purement « agents Web locaux » dans laquelle le contrôle des accès se positionne sur les serveurs des applications à protéger ;
- Remote agents Web » dans laquelle le contrôle des accès se positionne dans une passerelle et est dédié à une seule application et serveur Web. Cette architecture est privilégiée quand les applications à protéger sont complexes ou génèrent beaucoup de requêtes ;
- mixte « agent Web » / « passerelle » dans laquelle, en fonction de la politique de sécurité, de l'architecture réseau et applicative et de l'optimisation des flux réseaux, les points de contrôle peuvent se positionner soit en rupture soit sur les serveurs.

Architecture Web Agents de Web Access Manager



Des autorisations dynamiques

Les autorisations d'accès aux URLs et aux applications peuvent être calculées de manière dynamique en utilisant des règles simples du type « And », « Or » ou « Not » appliquées aux attributs de l'utilisateur disponibles dans l'annuaire LDAP. Ces règles sont définies de manière centralisée par l'administrateur puis appliquées par les modules de contrôles des accès.

Authentification de l'utilisateur

Web Access Manager peut authentifier les utilisateurs via différents moyens comme :

- un identifiant et un mot de passe ;
- un clavier virtuel permettant à un utilisateur de fournir son identifiant et son mot de passe en cliquant sur un clavier positionné aléatoirement à l'écran. Ce clavier virtuel offre une protection supplémentaire contre les « key loggers » sans nécessiter de périphérique ou de logiciel supplémentaire ;
- un mot de passe à usage unique OTP (One Time Password) :
  - calculé par un token,
  - envoyé par SMS,
  - envoyé par mail,
  - calculé par l'application smartphone QRentry à partir d'un QR code.
- une carte à puce avec certificat X.509 ;
- un jeton Kerberos (domaine Windows) ;
- un jeton SAML (Service Provider / Identity Provider) ;
- un moyen d'authentification basé sur le protocole radius ;
- une carte matricielle individuelle (Grid Card) permettant à chaque utilisateur de résoudre un challenge non rejouable ;
- des mécanismes d'authentification externes comme CAS, OpenID, OAuth (authentification par Facebook, LinkedIn, Twitter, Google+) ou le couplage avec n'importe quel mécanisme externe en utilisant le SDK Web Access Manager.

Superviser l'activité des utilisateurs

Toute politique de gestion d'accès requiert un contrôle. Web Access Manager suit tous les accès des utilisateurs ou toutes les tentatives d'accès afin de protéger les ressources Web, permettant ainsi aux administrateurs de savoir qui a accédé à quelle application et quand.

Web Access Manager est compatible avec les outils d'analyse de connexion tel que NetIQ WebTrends, afin de simplifier l'analyse des rapports d'audit de sécurité faite par les administrateurs.

Administration simple et rapide de multiples accès Web

- séparation entre l'infrastructure de sécurité et les applications ;
- solution non intrusive sur les serveurs qui ne demande pas de développements spécifiques ;
- capacité de montée en puissance pour suivre l'évolution du système d'information.

Chiffrer les données confidentielles

Pour garantir la confidentialité des données échangées sur Internet, les partenaires doivent ouvrir des sessions chiffrées. Comme de plus en plus d'entreprises travaillent désormais en ligne, le chiffrement de chaque application Web devient problématique, car toutes les applications ne permettent pas le chiffrement.

Avec Web Access Manager, toutes les communications avec le navigateur peuvent être chiffrées. Les clients, employés et partenaires peuvent dialoguer en toute confiance au sein de la communauté de sites gérés par Web Access Manager.

Protéger les ressources du Web contre les attaques

Web Access Manager aide à prévenir les attaques des ressources Web exposées sur Internet.

Les passerelles Web Access Manager cachent l'adresse réelle des ressources Web. Cela modifie l'URL des applications Web pour empêcher les pirates de connaître la topologie du réseau.

Web Access Manager contrôle également les entrées pour tous les accès Web. Cela facilite la protection des applications Web nécessitant un code d'accès contre les vers ou toute autre attaque provenant d'Internet.

Création des comptes utilisateurs

Web Access Manager s'intègre de manière cohérente dans les processus de gestion des utilisateurs existants.

Utilisation des annuaires LDAP de l'entreprise

Web Access Manager réutilise la définition des utilisateurs de l'entreprise dans les différents annuaires LDAP de l'entreprise. Les annuaires LDAP peuvent être de fournisseurs différents, avoir des schémas différents et résider sur des sites différents.

Création du compte par l'utilisateur

En fonction de la politique de sécurité mise en place, l'utilisateur peut être autorisé à créer son propre compte dans un annuaire LDAP prédéfini en se connectant à Web Access Manager. Son compte peut alors être intégré par un administrateur à la politique générale de contrôle des accès de l'entreprise.

Réinitialisation du mot de passe primaire

Lorsque l'utilisateur a oublié son mot de passe primaire, Web Access Manager lui offre la possibilité de réinitialiser ce mot de passe grâce à l'utilisation d'un formulaire de type question/réponse. L'utilisateur n'a pas besoin de faire appel au « help desk ». La politique de création des mots de passe définie par l'entreprise (nombre de caractères, non réutilisation d'un mot de passe déjà utilisé...) est alors appliquée.

Prise en compte des identités multiples

Un utilisateur peut avoir accès à de multiples domaines sous le même nom. Chaque identité est alors définie dans un annuaire LDAP différent. Nous parlons alors de domaines différents.

Ces différents domaines peuvent par exemple correspondre à des entreprises, filiales ou organisations différentes.

Web Access Manager permet à l'utilisateur de choisir son domaine lors de l'authentification initiale. Il hérite alors des droits associés à l'identité du domaine qu'il a choisi.

SSO universel

Les solutions de sécurité traditionnelles perturbent l'efficacité et le confort des utilisateurs. Pour sa part, Web Access Manager repose sur une approche simplifiée qui renforce la fidélité des utilisateurs. En facilitant la navigation par la connexion unique et en améliorant le confort des utilisateurs grâce à des contenus personnalisés, Web Access Manager optimise leur productivité et leur confiance.

Web Access Manager gère la connexion aux applications traditionnelles Web utilisant chacune leur propre mot de passe, aux applications utilisant le mot de passe du domaine telles que OWA, aux applications utilisant le protocole SAML.

Améliorer le confort des utilisateurs et la sécurité via une authentification unique

Lorsque les utilisateurs doivent fournir un mot de passe à chaque fois qu'ils veulent accéder à une application interne ou externe, la mise en oeuvre de la sécurité entrave forcément leurs activités. La gestion de multiples informations d'authentification est une activité frustrante qui prend beaucoup de temps.

Pour aller plus vite, les utilisateurs choisissent des mots de passe faciles à détecter ou les laissent à la vue de tous.

Les appels liés à des problèmes de mot de passe qui sont adressés au « help desk » représentent une part importante des coûts de ce service. La multiplication des mots de passe entrave non seulement les activités, mais elle génère également des failles de sécurité.

Avec Web Access Manager les clients, partenaires ou employés accèdent aux ressources Web internes et externes avec un seul nom d'utilisateur et un seul mot de passe. Après la procédure d'authentification initiale effectuée par Web Access Manager, ils peuvent naviguer librement parmi les ressources auxquelles ils sont autorisés à accéder. Transparent pour l'utilisateur, Web Access Manager fournit à chaque application l'identifiant et le mot de passe appropriés, notamment par l'intermédiaire des formulaires.

L'authentification unique vers des sites Web extérieurs

L'activité des organisations s'étendant au-delà du pare-feu vers des domaines multiples, le SSO doit également suivre le même chemin : les portails Intranet offrent souvent l'accès à des sites Web d'achat ou des services d'abonnement et l'Extranet peut couvrir plusieurs sites partenaires.

Avec Web Access Manager, les gestionnaires de portail peuvent contrôler leur environnement Web en ajoutant et en déplaçant des ressources de façon dynamique. Les utilisateurs peuvent accéder aux ressources à distance de l'entreprise sans être obligés de fournir un autre mot de passe.

La solution Web Access Manager améliore la sécurité, la satisfaction des utilisateurs et réduit le nombre d'appels adressés au « help desk ».

Web Access Manager est aussi la porte d'accès unique vers les applications en mode SaaS ou Cloud. La liste des services Cloud/SaaS est proposée directement dans la page d'accueil personnalisée de l'utilisateur et la même authentification primaire est utilisée vers ces applications grâce au protocole de fédération SAML.

Personnaliser l'environnement Web de l'utilisateur final

Parce que la navigation sur le Web est impersonnelle, les utilisateurs ont souvent des liens non pertinents sur leur page d'accueil. Web Access Manager personnalise cette navigation en donnant aux utilisateurs le sentiment d'appartenir à une communauté. Avec Web Access Manager, les utilisateurs de certains secteurs de l'industrie situés dans des zones géographiques prédéfinies peuvent obtenir un accès et des informations personnalisées. Les accès aux services des clients et partenaires sont sécurisés à plusieurs niveaux. En effet Web Access Manager a la capacité de répondre aux besoins des utilisateurs afin qu'ils se sentent membres d'une communauté sécurisée. L'authentification unique vient renforcer ce sentiment en permettant aux utilisateurs de naviguer de façon transparente au sein des applications autorisées.

L'utilisateur peut choisir de gérer lui-même les mots de passe sensibles

Les mots de passe peuvent être mis à jour, soit par un administrateur central, soit par un utilisateur. Si le mot de passe est géré par l'utilisateur, l'administrateur ne pourra pas y avoir accès.

Les accès à un compte commun

Plusieurs utilisateurs peuvent partager un compte commun sur une application cible.

Les mots de passe de groupe peuvent être transparents pour les utilisateurs finaux. Ainsi, un administrateur peut autoriser les membres d'un groupe défini à accéder à des rapports d'analyste sans leur communiquer le mot de passe de l'entreprise concernée.

Extensible aux accès projets J2EE, SOA et Web Services

Grâce à l'architecture modulaire, le module SOA Access Manager étend les fonctionnalités de Web Access Manager en offrant une solution intégrée de SSO aux environnements J2EE, SOA et Web Services.

En s'appuyant sur un serveur d'authentification et d'administration commun, Web Access Manager et SOA Access Manager coopèrent pour offrir aux utilisateurs un Single Sign-On aussi bien pour les environnements Web que les environnements J2EE et Web Services.

Grâce aux technologies SAML, SOA Access Manager étend simplement les fonctions de contrôle d'accès de Web Access Manager pour interconnecter les portails ou applications Web aux serveurs J2EE ou aux Web Services internes et externes.

Extensible aux accès non-Web et aux applications propriétaires

Lorsque les applications n'ont pas toutes un accès Web, la solution Authentication Manager et Enterprise SSO pour les applications non-Web vient en complément de Web Access Manager afin de fournir une solution complète et intégrée pour sécuriser et simplifier les accès aux applications non-Web et les applications propriétaires.

Gardez le contrôle de la sécurité :

- l'administration centrale minimise les coûts et les tâches associés à la sécurité ;
- la flexibilité de l'administration permet d'ajouter ou de révoquer les droits d'un utilisateur en quelques clics ;
- l'audit central permet de suivre à la trace toutes les connexions.

La sécurité instantanée pour un faible coût d'acquisition

Avec Web Access Manager, il n'est pas nécessaire de sacrifier la commodité à la sécurité. Web Access Manager ne requiert aucune modification ou ajout de composant sur les postes de travail des utilisateurs ni aucune modification des systèmes cibles. Les autres solutions actuellement disponibles sur le marché sont extrêmement complexes, nécessitent des mois de mise en oeuvre et consomment de précieuses ressources informatiques.

Une solution non intrusive pour un déploiement simplifié

Grâce à son architecture non intrusive, Web Access Manager peut être déployé intégralement en quelques heures et permet à l'entreprise d'évoluer aussi rapidement que le marché. Web Access Manager est un Identity Provider qui permet à l'entreprise de mettre à disposition de ses utilisateurs un SSO aux applications cloud telles que Servicenow, Salesforce, Successfactor, Office365.

Une administration plus efficace

Web Access Manager permet aux administrateurs de portail ou de serveurs Web de gérer de manière transparente l'accès à n'importe quelle application Web sans avoir à déployer de logiciel ou à réorganiser les répertoires. Web Access Manager ne perturbe ni les processus d'administration en place ni les applications. Web Access Manager réutilise les annuaires utilisateurs LDAP existants pour appliquer une politique de sécurité sur les ressources de l'entreprise.

Vers la gestion des identités et des accès de votre portail « Corporate »

Evidian Identity & Access Manager permet une gestion complète du cycle de vie des identités et des accès aux services. En effet, Evidian I&AM s'appuie sur une gestion interne de la politique d'autorisation basées sur les rôles et les organisations de l'entreprise et un système complet de workflow, de provisionnement et de contrôle d'application de la politique sur les applications et services.

Un point de contrôle pour l'entreprise étendue

Le besoin d'un opérateur de télécommunications, qui a été développé dans ce livre blanc, est partagé par la plupart des entreprises ou des organismes qui doivent ouvrir leur système d'information à leur collaborateurs nomades et donc étendre leur entreprise.

- l'hôpital prévoit désormais l'accès à son système d'information pour les médecins de ville, des intervenants en milieu rural, etc.
- la communauté d'agglomérations ouvre des services d'inscription qui sont mis à disposition des agents territoriaux où qu'ils exercent : piscine municipale, cantines, etc.
- la compagnie d'assurance partage ses applications professionnelles avec son réseau de courtage.

Les principes et recommandations qui sont exposés dans ce document, sont génériques et transposables pour ces nombreux cas d'usage professionnels.

La suite logicielle Evidian

Notre solution IAM est reconnue par les clients et les analystes pour sa complétude. En effet, elle offre les composants suivants, pouvant être déployés indépendamment ou intégrés nativement :

- **Evidian Identity & Access Manager** permet la gouvernance des autorisations et une gestion complète du cycle de vie des identités et des accès aux services, pilotée par une politique de sécurité et ses workflows d'approbation.
- **Evidian Web Access Manager** fédère des accès aux applications web, sécurise l'accès des utilisateurs mobiles et remplace l'ensemble des mots de passe des utilisateurs par un mode d'authentification unique et forte.
- **Evidian Enterprise SSO** gère l'accès aux applications d'entreprise et personnelles sur les postes de travail ainsi que sur les terminaux mobiles, évite à l'utilisateur de mémoriser et saisir les mots de passe.
- **Evidian Authentication Manager** offre l'authentification forte sur les postes de travail et terminaux mobiles : carte ou token avec certificat, carte sans contact, biométrie, mot de passe à usage unique.
- **Evidian SafeKit** apporte la haute disponibilité et le partage de charge aux applications.

Prérequis au RGPD*

La Gestion des Identités et des Accès est un élément parmi l'ensemble des mesures techniquespermettant de mitiger les risques liés à le protection des données.
En plus de ses fonctionnalités de contrôle des accès, d'authentification forte et de gouvernance des identités, la Suite Evidian prend en compte les obligations du droit à la personne dans ses solutions. Des fonctionnalités de notification, le libre-service et des rapports dédiées permettent l'exercice des droits utilisateurs et des processus conforme au RGPD.

*Règlement Général sur la Protection des Données

À propos d'Evidian

Evidian est la suite logicielle de gestion des identités et des accès (IAM), d'Eviden.

Evidian IAM est le leader européen des logiciels de gestion des identités et des accès, avec une présence en pleine croissance en dehors du continent européen et notamment aux Etats-Unis et au Japon.

Plus de 5.000.000 d'utilisateurs dans plus de 900 organisations dans le monde entier se connectent tous les jours à leur entreprise et gèrent leurs droits d'accès avec les solutions de gestion des identités et des accès d'Evidian.

CT_J1306_180626_RY_B_NOMADISME