

Evidian Identity Governance and Administration

06-2021

Trusted partner for your Digital Journey

© Atos - Confidentiel

Atos

Introduction



110,000 experts
dans 73 pays



12 Mds € de chiffre d'affaires &
1,2 Md € de marge opérationnelle



Partenaire informatique des
Jeux Olympiques



Leader Mondial du **cloud** et de
l'espace de travail digital



N ° 1 des **services de sécurité gérés** en Europe
et **n ° 3** au niveau mondial



235 M € de R&D
4500 brevets par an



52,000 nouvelles
certifications numériques



20.97tCO₂/m€ de
revenus de l'industrie,
meilleur de sa catégorie

BDS Digital Security Portfolio

DIGITAL SECURITY

Integrated Solutions, Large security Systems

Mission-critical systems

Critical communications solutions
Command, control & intelligence
Aerospace & defense electronics

Cybersecurity products

Digital Identities
Identity & Access management
Data protection

Cybersecurity services

Security advisory & integration
Managed security services



LEADER

LEADER

Number 3

LEADER



Managed Security
Services Europe



Cyber Resiliency Services
& GDPR Services WW



Managed Security
WW Market share



Identity
Provisioning Global

Editeur Logiciels de solutions de Gouvernance des Identités et des Accès

- Access Management
- Identity Governance
- On premise, As a Service, Managed Services

Gartner



Références mondiales

- Europe, Japon, Amérique du Nord, MEA
- +900 clients , +5 millions d'utilisateurs professionnels
- R&D en Europe

Partenariats Technologiques et interoperabilité



Suite de Gestion des Identités et des Accès

La base d'une sécurité centrée sur l'activité



Identity Governance & Administration

Gouvernance, gestion et contrôle des identités :
arrivants – évolutions – sortants
Gestion de la politique
Processus et droits d'accès
Provisioning
Recertification - Réconciliation



Web Access Manager

Fédération des identités,
autorisation basée sur la politique,
SSO Web et authentification
multi-facteur



Enterprise SSO

Accès sécurisé aux applications par
mots de passe depuis PC, tablettes
et smartphones



Authentication Manager

Authentification Windows multi-
facteur et orientée métier, SSPR



SafeKit

Répartition de charge, réplication
synchrone des fichiers au niveau
octet, reprise sur incident



Analytics and Intelligence

Conformité durable, analyse des
risques et analyses avancées
des identités et des accès



IDaaS - Identity as-a-Service

Fédération d'identité
MFA pour applications WEB

**Gestion des identités
et des accès**

**Authentification
multi-facteur**

**Fédération des identités
authentification web**

**Réinitialisation du mot
de passe en libre-service**

SSO universel

Continuité de l'activité

Références par marché, à l'échelle mondiale

5 M +
d'utilisateurs

Finance Service	Industrie, Vente de détail, Transport	Télécommunications Médias, Utilities	Publique Santé

Conformité

Exigences IAM et RGPD d'Evidian

Exigences GDPR	Suite Evidian IAM			
	IGA	Analytics & Intelligence	Enterprise Access Management	Web Access Management
			E-SSO	Authentication Manager
Accès aux données	Accès via interface libre service	Contrôle d'accès basé sur les rôles (RBAC)	Accès via interface libre service	Accès via pages libre service
Modification & Suppression	Interface libre service pour modifications et suppression	Pseudonymisation automatique après une période de rétention	Interface libre service pour modification et suppression	Suppression sur demande et après inactivité
Limitation de traitement	Demandes de limitation ou suspension avec le mode «Départ d'utilisateur»	Contrôle du traitement selon la politique IGA	Possibilité de désactiver/réactiver des comptes	Désactivation/Réactivation
Notifications & consentement	Propagation automatique par provisionnement/déprovisi.	Rapports de consentement	Envoi d'email lorsque le mot de passe SSO primaire est changé.	Outil Pop-Up automatisé de gestion du consentement
Portabilité des données	Données transférables via API	Données transférables	Possibilité de recevoir ses comptes SSO par email et de les révéler depuis le poste de travail ou depuis le portail Web	Export de données via pages libre service
Sécurité du Traitement	Pseudonymisation des événements d'audit, compatible avec Atos HSM	Pseudonymisation des rapports, RBAC	Pseudonymisation des événements d'audit, compatible avec Atos HSM	Pseudonymisation des événements d'audit, compatible avec Atos
Gouvernance basée sur le risque	Approche basée sur le risque avec outil de recertification.	Rapports ad hoc	Méthodes d'authentification fortes adaptées à chaque niveaux de risque	Authentification forte adaptative
Audit & Contrôle	Accès aux événements d'audit via console	Rapports et tableaux de bords comme preuve de conformité	Accès aux événements d'audit (jour/semaine/mois). Rapports et tableaux de bords	Accès à l'historique des événements d'audit

Evidian Identity Governance and Administration

Le cœur de la gestion des identités

Qui a accès à quoi ?

Est-ce légitime ?

Pouvez-vous le prouver ?



**Gestion des Identités
et des Comptes**

**Politique de Sécurité
/ Conformité**

**Processus / Rapports
/ Revue de comptes**

Automatisation

Gouvernance

Evidian Identity Governance & Administration

Automatisation

Gestion du cycle de vie des utilisateurs et des organisations

Constitution d'un annuaire centralisé
Gestion des organisations et ses évolutions
Arrivées/Départs/Mutations

Connecteurs de provisionnement
Intégration avec outil de ticketing
Création de comptes dans les applications

Gestion des accès et droits dans les applications

Gouvernance

Politique d'attribution des droits et conformité (RBAC)

Politique basée sur rôles et organisations
Vérification des accréditations nécessaires
Administration centralisée ou distribuée

Portail libre-service / Processus Workflow
Campagnes de revue de comptes
Rapports : auditeurs/réglementations

Processus de gestion, éléments de gouvernance



Multiples sources
d'identités

Doublons

Arrivées / Départs /
Mutations

Retour / Période de longue
absence

Opérations unitaires ou
en masse

Changement de la structure
organisationnelle

Automatisation

Gestion du cycle de vie des utilisateurs et des organisations

Constitution d'un annuaire centralisé incluant tous les utilisateurs

Tout type de source d'identité : systèmes RH, annuaires LDAP, SQL, fichiers CSV/ XLS, Web Services, ...

Lancement automatique des workflows de gestion des utilisateurs et d'assignation des droits

Processus dédiés à la gestion des organisations et aux conséquences des évolutions dans les droits des utilisateurs

Fonctions de simulation et gestion de seuils

Automatisation

Création automatique
des comptes en fonction
du profil utilisateur

Application immédiate des
décisions sur les droits

Élimination des erreurs
humaines

Gestion des comptes et
mots de passe par
l'utilisateur final

Gestion des accès et droits dans les applications

Plusieurs processus de provisionnement proposés :

- Demande de validation au propriétaire d'application
- Capacité à compléter manuellement les données à provisionner
- Capacité à lancer des actions Post-Provisionnement

Gestion des multi-comptes

Provisionnement des applications Cloud à coût optimisé.

Sans connecteur :

- Demande par workflow au responsable d'application
- Création d'un ticket dans un système de ticketing

Connecteurs dédiés : AD, Exchange, Salesforce, ServiceNow, GSuite, Azure/Office 365, TEAMS, CRM, SAP, IBM RACF, Lotus Notes, OpenStack, Box, Oracle Fusion, CyberArk, Wallix, ...

Connecteurs génériques: LDAP, SQL, Web Services, CSV, JAVA

Politique d'attribution des droits et règles de conformité

Basée sur un modèle RBAC étendu, avec des organisations, des contextes et des règles métier

Assignation dynamique de rôles à partir de valeurs d'attributs utilisateur

Vérification et suivi du respect des accréditations requises pour l'affectation d'un droit

Règles de séparation des tâches

Administration centralisée ou distribuée

Fonctions de simulation, espace de travail

Définir qui accède à quoi et qui fait quoi

Respect et suivi des contraintes de conformité

Suivi des évolutions des droits selon le métier

Gestion des risques

Processus de gestion, éléments de gouvernance

Acteurs des workflows & nombre d'approbations basés sur la politique de sécurité

Pages construites dynamiquement en fonction des droits de l'utilisateur

Campagnes de revues de comptes par utilisateur ou par application

Processus de réconciliation pour détecter les écarts

+ 100 Rapports disponibles en différents formats (PDF, Excel, CSV) signés, planifiables, envoyés par mail

Droits d'édition gérés par des permissions

Processus de gestion des identités et des droits prêts à l'emploi

Portail libre-service : gestion des habilitations déléguée au métier

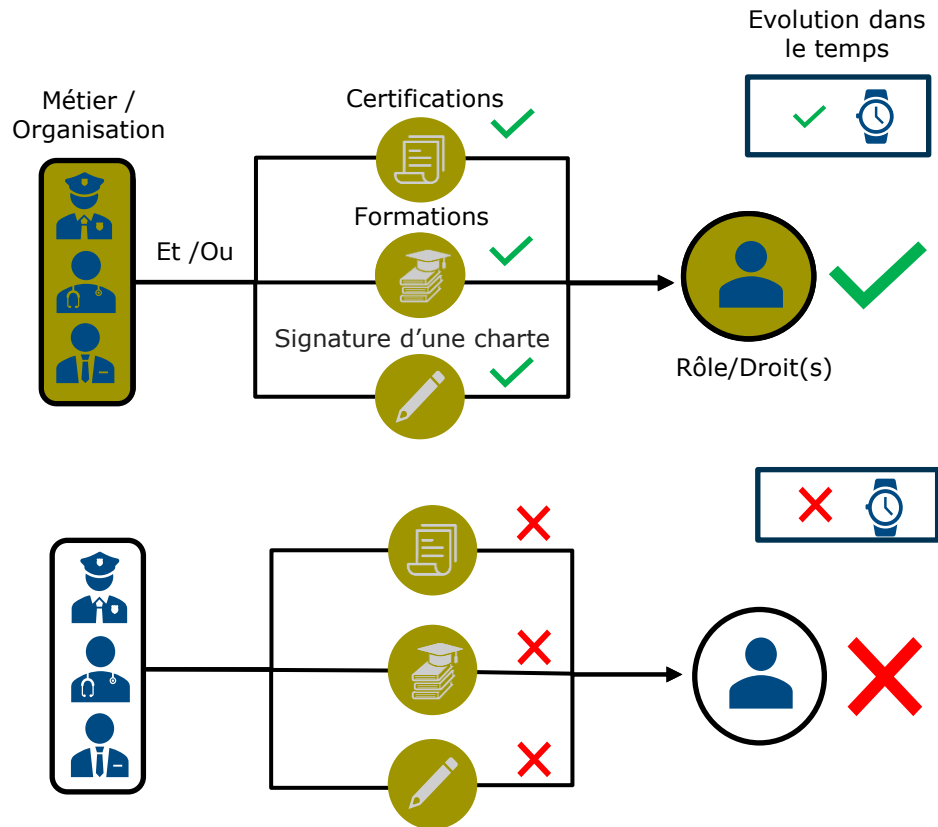
Revue de comptes pour assurer le principe du moindre privilège

Rapports pour auditeurs et réglementations

Gouvernance : Assignations conditionnelles

Contrôle des accréditations requises

- ▶ Certains rôles / droits requièrent avoir un niveau d'accréditation valable
- ▶ Vérification de la validité des accréditations lors de l'assignation
- ▶ Prise en compte dynamique des évolutions du niveau d'accréditation
- ▶ Révoquer dès l'expiration de l'accréditation et inversement



Gouvernance : Revue de comptes

Assurer le respect du principe du moindre privilège

Définition des paramètres de campagne



- Cible les utilisateurs ou les applications
- Sélection du niveau de risque des droits ou applications à recertifier

Phase de revue



- Approuver ou révoquer les droits
- Enregistrement des actions

Remédiation



- Validation ou modification des décisions de revue
- Application automatique des décisions

Application automatique des décisions



- Les décisions sont appliquées sur les systèmes cible
- Notification à l'utilisateur

Suivi des processus



- Vue sur le statut de la campagne
- Possibilité de forcer le passage à l'étape suivante

Rapports et archivage



- Rapports dédiés
- Possibilité d'abandonner et de supprimer les campagnes en cours

Gouvernance : rapports prédéfinis

Outils de conformité

Etat de la politique - Administrateurs des applications - Assignations : - Rôles - Applications - Permissions - Demandes de droits - Modèle de la politique - Rapport sur les organisations	RGPD - Activité utilisateur - Comptes utilisateur - Droits utilisateur - Informations d'identité	Indicateurs Qualité - Accès non conforme à la politique - Avertissements sur le modèle de la politique - Comptes orphelins - Indicateur de la qualité des assignations - Permissions sans rôle/utilisateur - Informations détaillées sur les écarts de réconciliation - Rôles sans permission - Rôles sans utilisateur - Utilisateurs sans rôle/permission
Activité - Accès utilisateurs - Accès échoués - Authentifications réussies - Comptes dormants	Statistiques - Statistiques sur les durées de traitement des droits - Répartition des assignations de rôles - Statistiques sur les applications métier - Répartition des assignations d'applications métier aux utilisateurs - Statistiques sur les permissions : - Statistiques sur les demandes d'accès - Statistiques sur les rôles - Synthèse des durées de traitement des demandes de droit	
Cycle de Vie Utilisateur - Arrivées utilisateurs - Départs utilisateurs		Recertification - Liste des campagnes de recertification - Campagnes de recertification classées par acteur/application - Droits recertifiés par application/utilisateur - Détails d'une campagne de recertification - Résumé des campagnes de recertification

Gouvernance : rapports prédéfinis

Rapports pour la conformité SOX

Pour chaque application

- **Attributions des permissions utilisateurs**

Liste des permissions et de leurs attributions aux utilisateurs

- **Statistiques sur les assignations des applications**

Répartition des habilitations : applications et utilisateurs

- **Comptes utilisateurs**

Liste des comptes utilisateurs utilisés pour se connecter aux applications

Pour chaque utilisateur

- **Droits utilisateurs**

Liste des applications auxquelles l'utilisateur peut accéder

- **Permissions utilisateurs**

Liste des utilisateurs et de leurs permissions

- **Accès utilisateurs**

Liste des accès utilisateurs à partir d'une date donnée

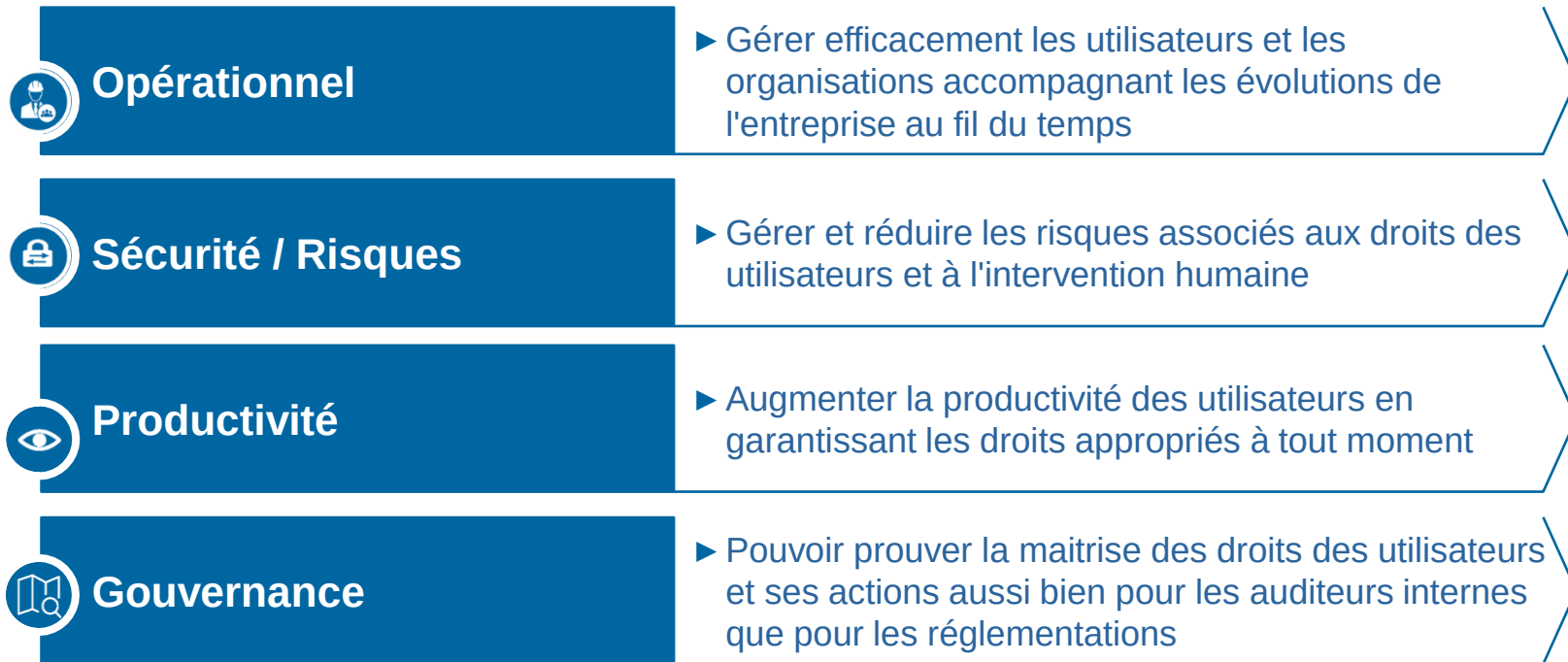
Pour chaque définition de rôle

- **Modèle de politique de sécurité**

Vous pouvez générer plusieurs types de rapports liés à votre modèle de politique de sécurité

- **Avertissements sur le modèle de la politique**

Ce rapport donne la liste des permissions attribuées directement aux utilisateurs



Evidian Analytics & Intelligence

Proposition de valeur

Evidian Analytics and Intelligence enrichit les avantages de l'Identity and Access Management



Contrôle l'utilisation de l'IAM

Statistiques sur l'utilisation des processus IAM

Vues des données en fonction du périmètre

Contrôle d'accès à la donnée

Détection des risques

Identification des pratiques suspectes

Données de conformité et d'historique

Preuve de gestion et possibilité de voir les valeurs des objets dans le passé

Recherche sur les événements et analyse des tendances

Analyse et audit combinant à la fois les données de politique et d'utilisation

Superviser l'utilisation et les tendances



Collecte de données
Avec la Suite IAM d'Evidian



Transformation

- Enrichissement des données
- Étiquetage pour contrôle d'accès à la donnée
- Vues orientées métier



Analyse

- Tableaux de bord
- Rapports
- Vues Ad-Hoc
- Historique des données



Risques et tendances

- Analyse de risque
- Événements suspects
- Analyse des causes racines

**Gouvernance
optimale**

Préparation des données

Domaines métier pré-définis

Etiquetage des événements d'audit et des objets pour le contrôle d'accès à la donnée

Accès aux données

Tableaux de bord, vues ad hoc, rapports pour visualiser et analyser l'évolution des données sur différents critères

Historique des données pour voir les valeurs des objets à un moment donné dans le passé

Interface graphique conviviale pour analyser la base d'audit facilitant **l'analyse des causes racines**

Fonctions de « glisser / déposer » pour faciliter la **personnalisation et la création**

Droits d'accès aux données de l'utilisateur définis dans la politique de sécurité d'Evidian IGA

Domaines

Visualiser les données et les tendances



Evidian A&I comprend une gamme de domaines prédéfinis:

- **Authentifications des utilisateurs**
- **Risque d'authentification pour les utilisateurs**
- **Utilisateurs**
- **Accès aux applications**
- **Utilisateurs avec violations SoD**
- **Utilisateurs sans droits**
- **Demandes d'attribution / de révocation de droits**
- **Cycle de vie des utilisateurs**
- **Changements de mot de passe**
- **Échecs de provisionnement**
- **Inscription / désinscription utilisateur-service**

Tableaux de bord

Visualiser les données et des tendances

- **Tableaux de bord:** Focus sur un indicateur de performance donné



Questions ?



Merci

For more information please contact:

T+ 33 1 30806230

M+ 33 6 70761477

jordi.cuesta@atos.net

IGA Product Manager

Atos, the Atos logo, Atos|Syntel are registered trademarks of the Atos group. November 2020. © 2021 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.

The Atos logo, featuring the word "Atos" in a bold, blue, sans-serif font. The letter 'o' is stylized with a white dot in the center.