

Evidian IDaaS Access

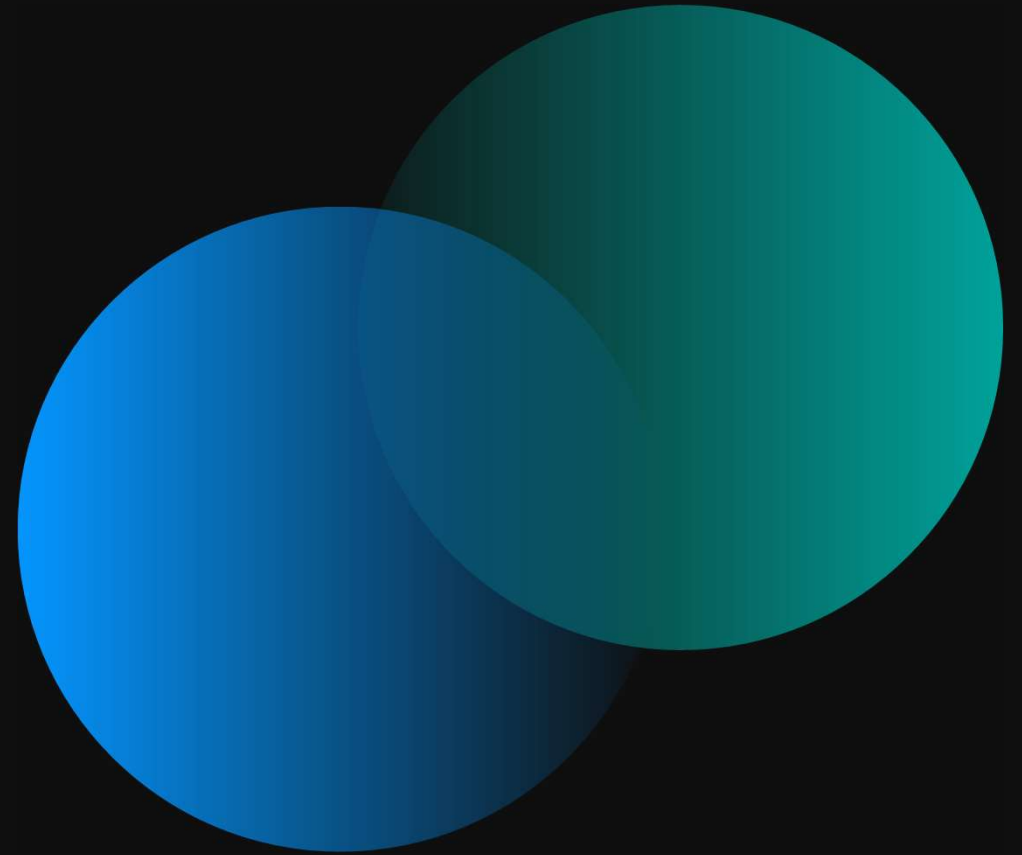
Yann Morvan Solution Manager
Franck Laloum Sales Manager



© Atos - For internal use

Atos

Introduction



Atos en résumé



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

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



Références par marché, à l'échelle mondiale



5 M +
D'utilisateurs

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

L'offre IAM d'Evidian en résumé



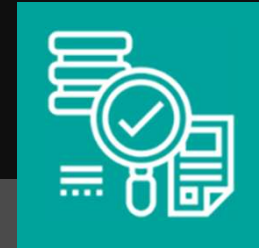
Identity Governance and Administration

Assurer une gestion facile du cycle de vie des identités numériques des utilisateurs et automatiser les processus liés aux utilisateurs et aux droits d'accès



Single Sign-On et Access Controls

Permettez aux utilisateurs de se connecter une seule fois et d'accéder à plusieurs services et ressources en toute sécurité, avec de nombreuses fonctionnalités MFA augmentant l'expérience utilisateur et réduisant les risques



Analytics

Améliorez la conformité de la sécurité avec des analyses avancées et de l'analyse de risques telle que les examens d'accès, les tableaux de bord approfondis

Formation - Services professionnels - Support - Global Delivery Center

Suite Identity and Access Management

La fondation pour une sécurité basée sur les métiers



Identity Governance & Administration

Gouverne, gère et contrôle les identités des utilisateurs
Approvisionnement -
Reconciliation
Recertification



Web Access Manager

Fédération d'identité, Web SSO
et authentification multifacteur



Enterprise SSO

Accès sécurisé aux applications
utilisant des mots de passe à
partir du PC ou Mobiles



Authentication Manager

Authentification multifactorielle
Windows pour les entreprises



SafeKit

Répartition de charges,
replication synchrone des
fichiers au niveau octet, reprise
sur incident



Analytics and Intelligence

Analyses avancées pour
l'Identité et l'Accès



Evidian IDaaS

Accès et Gouvernance

Gestion des identités et
des accès

Authentification
multifactorielle

Fédération d'identité
Authentification web

Libre-service
sécurisé

Single Sign-On
universel

Services gérés
On-Premise ou en
mode SaaS



Evidian IDaaS Accès

Inclus

- Gestion des accès et fédération
- MFA, Authentification forte.
- Gestion simple des utilisateurs intégrée
- Charge en masse d'utilisateurs
- Tableau de bord des applications des utilisateurs finaux

Modules complémentaires

- Personnaliser / Créer des rapports et des tableaux de bord
- Services (SSR, NSSR)



Evidian IDaaS
Accès

Inclus

- Gestion des accès et fédération
- MFA, Authentification forte.
- Gestion simple des utilisateurs intégrée
- Charge en masse d'utilisateurs
- Tableau de bord des applications des utilisateurs finaux

Modules complémentaires

- Personnaliser / Créer des rapports et des tableaux de bord
- Services (SSR, NSSR)



Evidian IDaaS
Gouvernance

Feuille de route

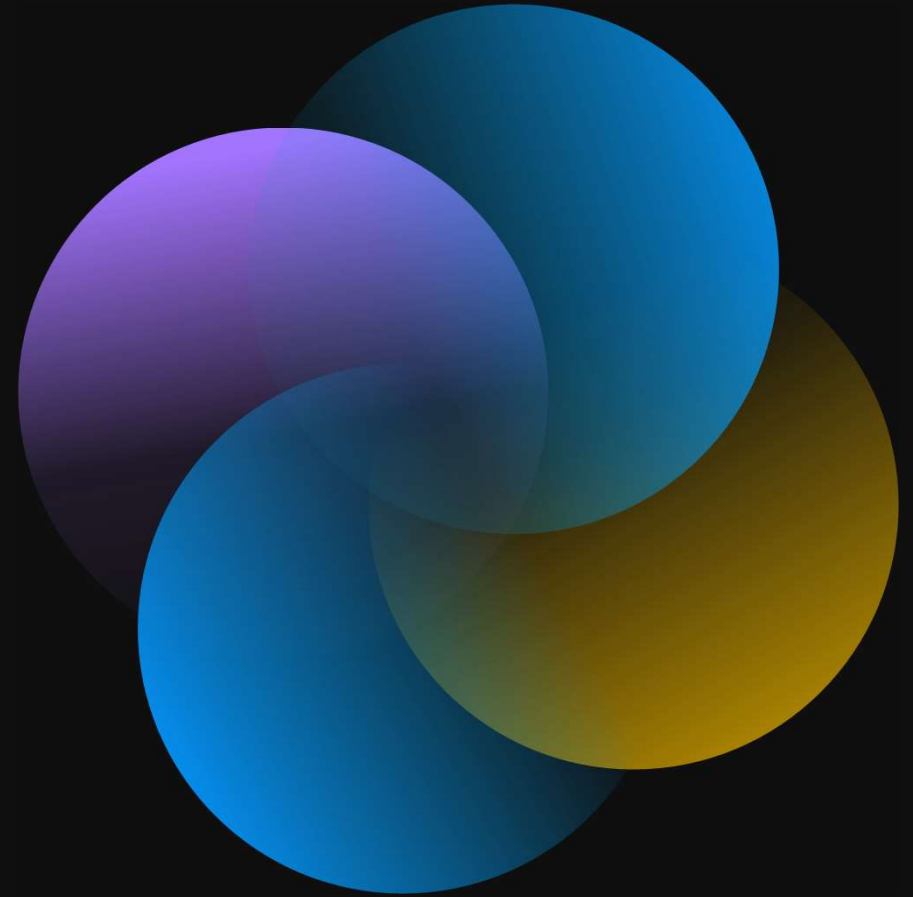
Inclus

- Processus avancé de gestion du cycle de vie des utilisateurs
- Provisionnement d'applications Cloud
- Charge en masse d'utilisateurs, d'organisations, de rôles et de politiques

Add-ons

- Campagnes de certification
- Services (SSR, NSSR)

Les challenges du « Cloud Access »



Qu'est ce que l'IAM?

Identity and Access Management



Assurez-vous que seules les bonnes personnes accèdent aux bonnes applications d'entreprise



- ▶ Intégration et validation des identités
- ▶ Entrants, évolutions, sortants de l'entreprise
- ▶ Travailleurs à domicile, partenaires...



- ▶ Application de l'accès avec MFA
- ▶ Authentifications adaptatives et contextuelles
- ▶ Travail au bureau ou à domicile



- ▶ SSO sécurisé
- ▶ Fédération d'identité
- ▶ Password Vault (coffre fort de mots de passe) pour les informations d'identification

Challenges de l'IAM

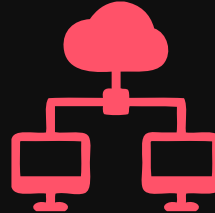


Sécurité

Mot de passe, MFA, contextuelle, accès externe, attaques par force brute...

80% de toutes les organisations

subissent au moins une menace de compte compromis par mois



Nouveaux usages

Travail à domicile, télétravail, itinérant, entreprises mondiales, BYOD, smartphones...

3 entreprises sur 4

laissent leurs employés utiliser leur propre appareil pour accéder aux applications professionnelles



Nouvel IT

SaaS, cloud, fédération d'identité, API REST, accès partenaires, CIAM...

70% des transactions SSO

émanent d'applications sur site à partir d'aujourd'hui, tandis que les protocoles de fédération modernes devraient représenter 60% d'ici 2022

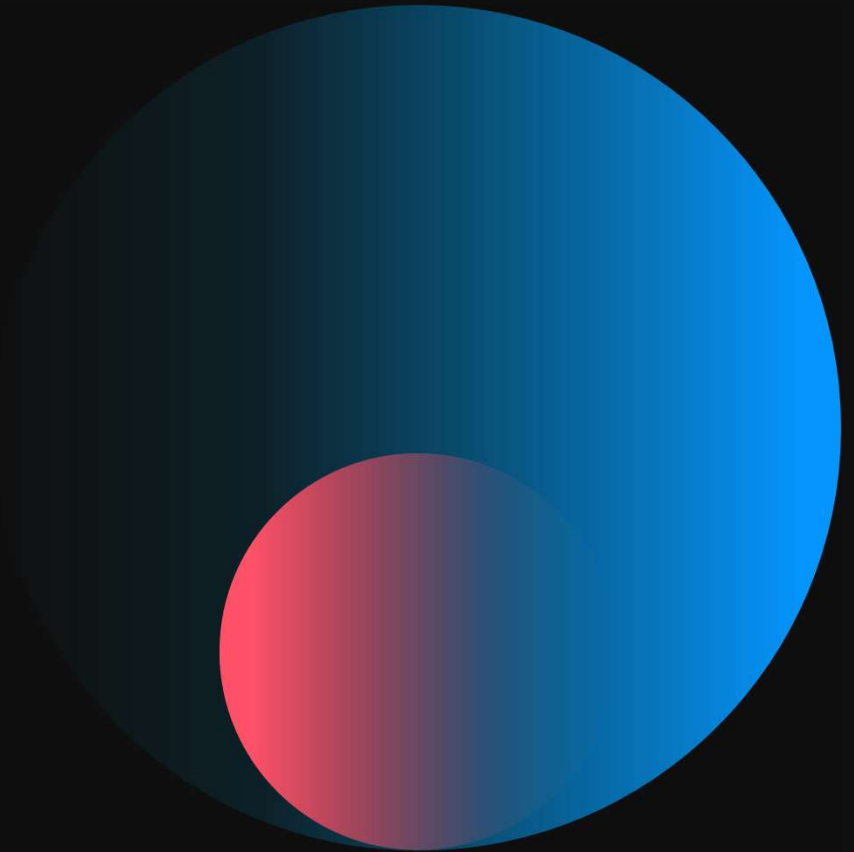


Les analystes et les études ont régulièrement constaté au cours des dernières années qu'environ

70%

des violations de données sont liées à des identifiants volés ou faibles

Evidian IDaaS



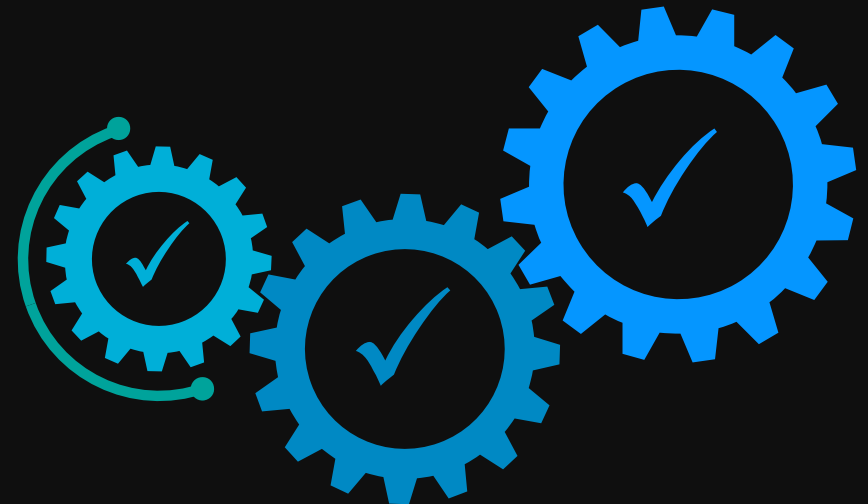
AtoS



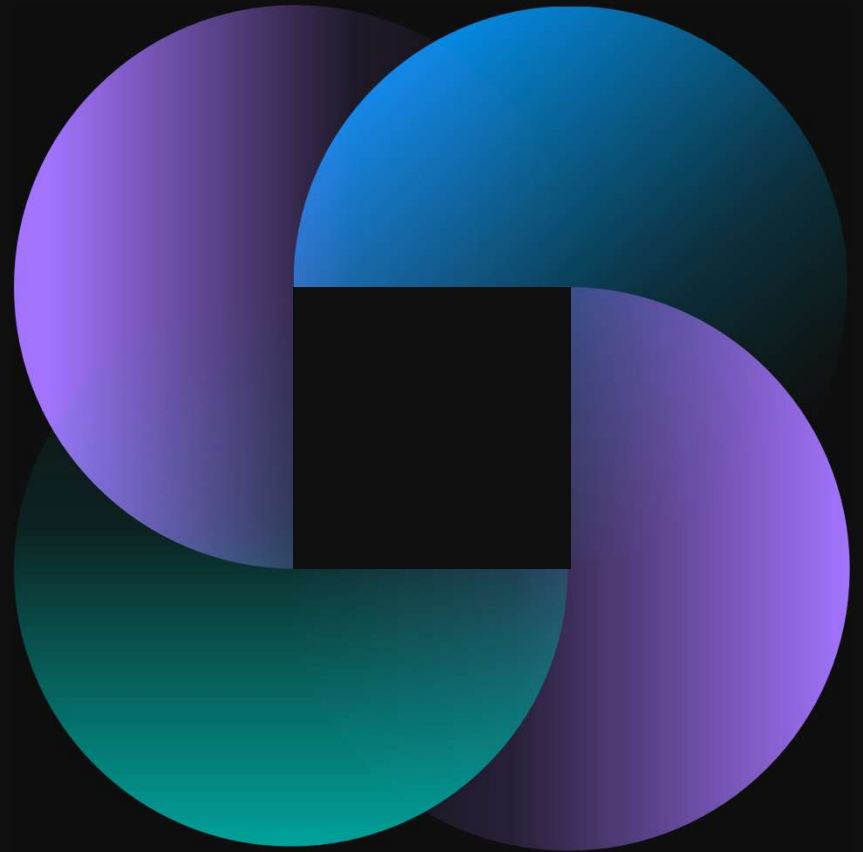
Evidian ID as a Service

Permet aux entreprises de gérer et de protéger l'accès de leurs utilisateurs à leurs applications et ressources cloud ou sur site :

- Synchronisation des identités
- Appliquer l'authentification multifacteur
- Protégez les nouvelles utilisations avec l'authentification unique et accédez de n'importe où



3.1 Applications préconfigurées



Modèles d'applications cloud et Web

- Plusieurs applications pré-intégrées de pointe avec une configuration facile pour un déploiement rapide
- Modèle SAML générique pour les applications personnalisées
- En continu, plus de modèles à venir

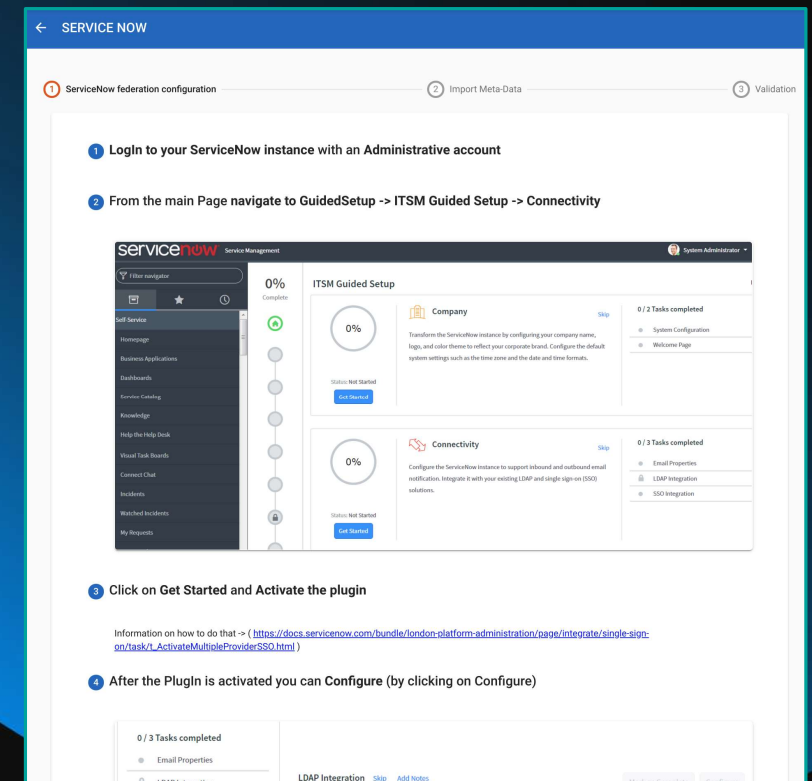
SAML APPLICATIONS		
	ADP Suite Payroll and HCM solution...	CONFIGURE
	Amazon Web Services Amazon Web Services off...	CONFIGURE
	Box Cloud content manageme...	CONFIGURE
	Google GSuite G Suite (formerly Google ...	CONFIGURE
	Microsoft Office 365 Collaborate with online ve...	CONFIGURE
	Salesforce A customer relationship ...	CONFIGURE
	Service Now Service Now was a softw...	CONFIGURE
	Webex Enterprise solution for vid...	CONFIGURE
	Workday A single system for financ...	CONFIGURE

Gestion des applications

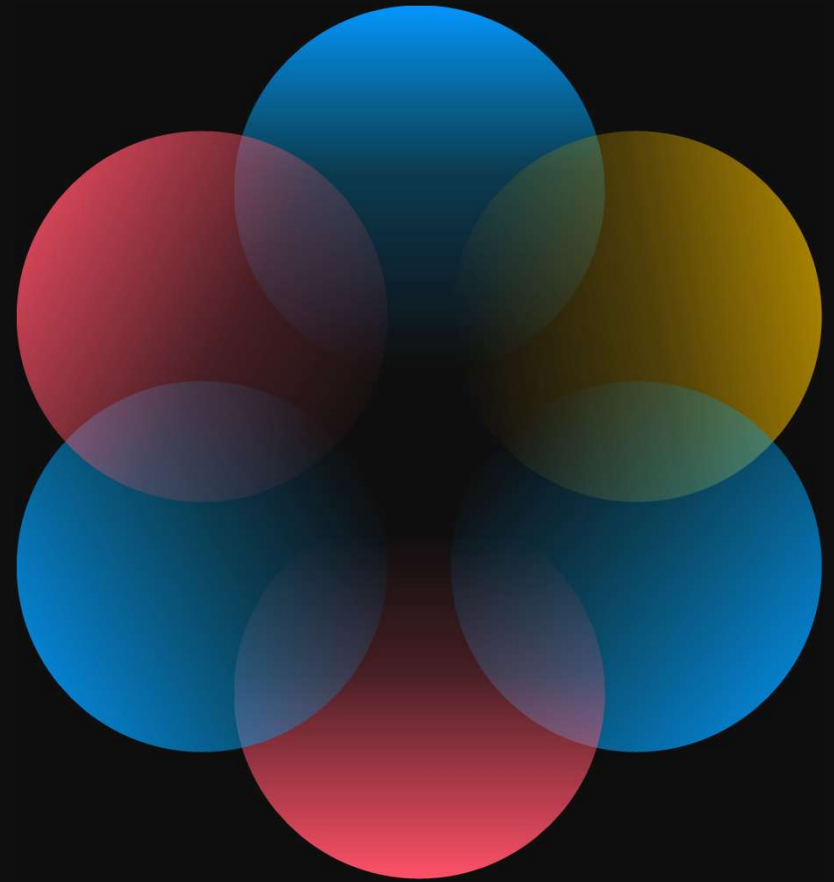


- Assistant de configuration guidé étape par étape
Lisez la documentation pendant que vous configurez
- Utilisez le modèle SAML générique pour ajouter des applications personnalisées
- Gérer vos applications Legacy ¹⁾

1) nécessite Evidian WAM et prof. services



3.2 Méthodes fortes d'authentification



Contrôle pour chaque méthode d'authentification disponible :

- **Contexte de l'utilisateur**
c'est-à-dire : Méthode d'authentification différente selon l'emplacement (au travail ou à la maison)
- **Définir la durée maximale avant une nouvelle authentification,**
c'est-à-dire : la ré-authentification est automatiquement demandée après une durée prédéfinie
- **Définir le délai d'inactivité maximal pour l'utilisateur,**
c'est-à-dire : l'authentification expire après un délai prédéfini si aucune action de l'utilisateur



Catalogue d'authentification prêt à l'emploi



Mot de passe simple désactivé par défaut pour plus de sécurité



Tous les deuxièmes facteurs (OTP, TOTP, FIDO, Grid) peuvent être utilisés comme méthodes autonomes



Les utilisateurs s'auto-inscrivent et gèrent les méthodes MFA (sauf certificat)



Authentification sociale et liaison de compte (Google, Windows Live, LinkedIn, ...)

+ Toute méthode d'authentification tierce¹⁾

+ Authentification Windows intégrée (IWA)²⁾

¹⁾ SAML ou OAuth based

²⁾ nécessite prof. services



Push Authentication

Use your phone and Evidian Authenticator



Password Authentication

Use your login and password



Password and Mail OTP authentication

Use your login password and an OTP sent by mail



Password and TOTP Authentication



Password and FIDO Authentication

Use your FIDO (WebAuthn) key



Password and Grid authentication

Use your login password and your personal Grid



Certificate Authentication

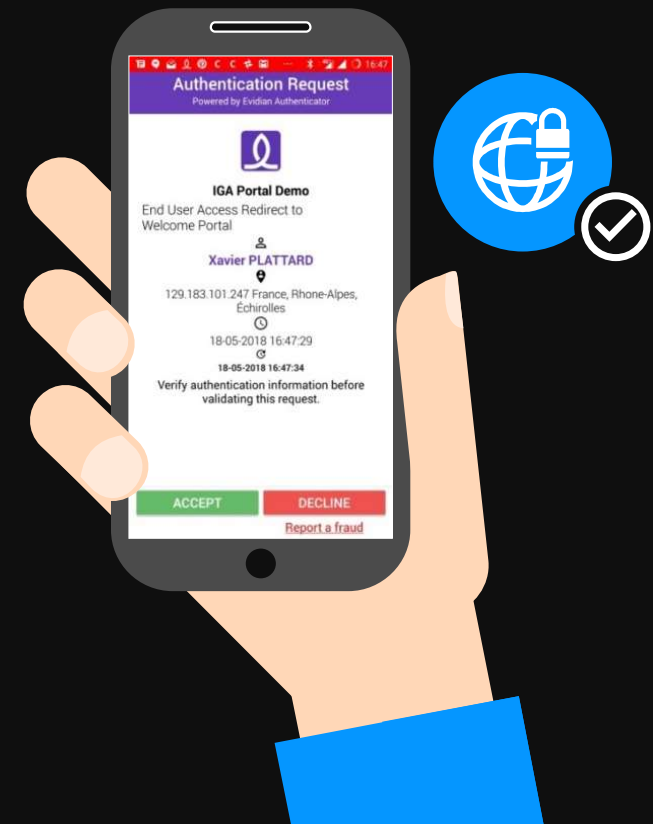
Use your certificate card

Renforcez la sécurité avec Evidian Authenticator

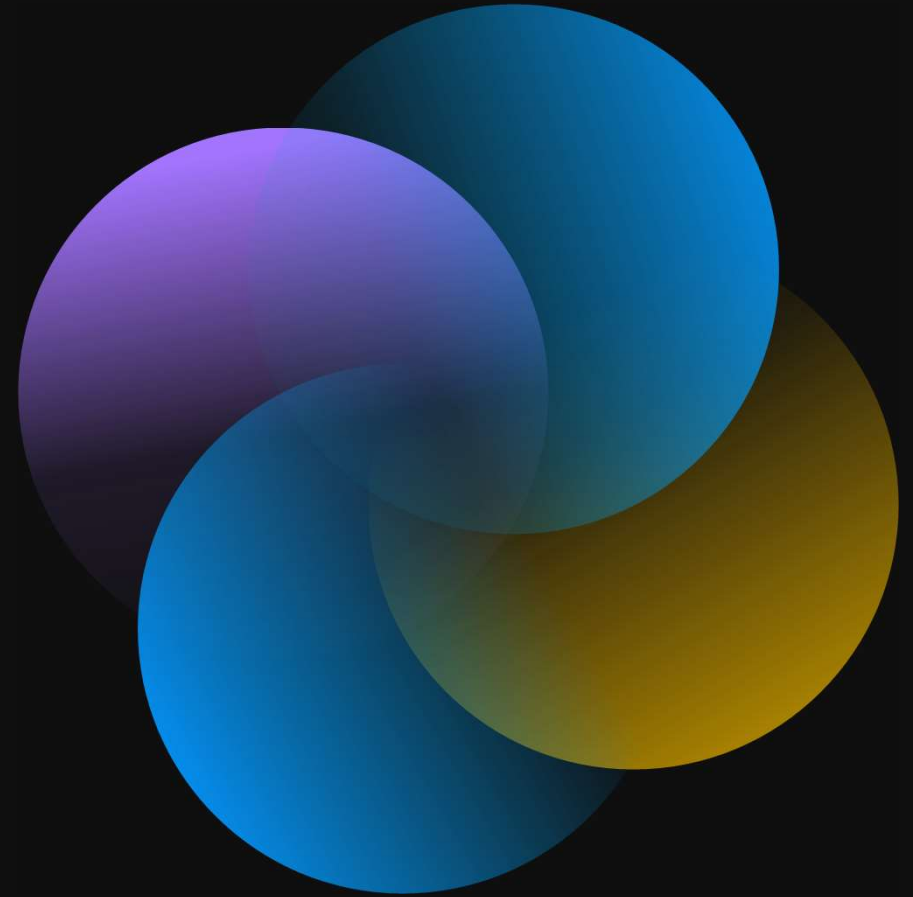


Y compris l'authentification mobile push avec l'application Evidian Authenticator

- Expérience utilisateur **sans friction**
Accepter la notification de demande
- **Sécurité** intégrée
Toujours demander un code PIN secret ou une empreinte digitale
- Fonctionne sur **Android** et **Iphone**



3.3 Utilisateurs



Gestion utilisateurs

- Activation de compte sécurisée pour imposer l'utilisation de **MFA** ou **2FA**
- Faites **glissez et déposez** le fichier CSV pour une importation utilisateur rapide et pratique
- Fonction de **recherche dynamique** multi-attributs
- **Verrouiller/déverrouiller** des utilisateurs
- **Créer, lire, mettre à jour et supprimer** des utilisateurs

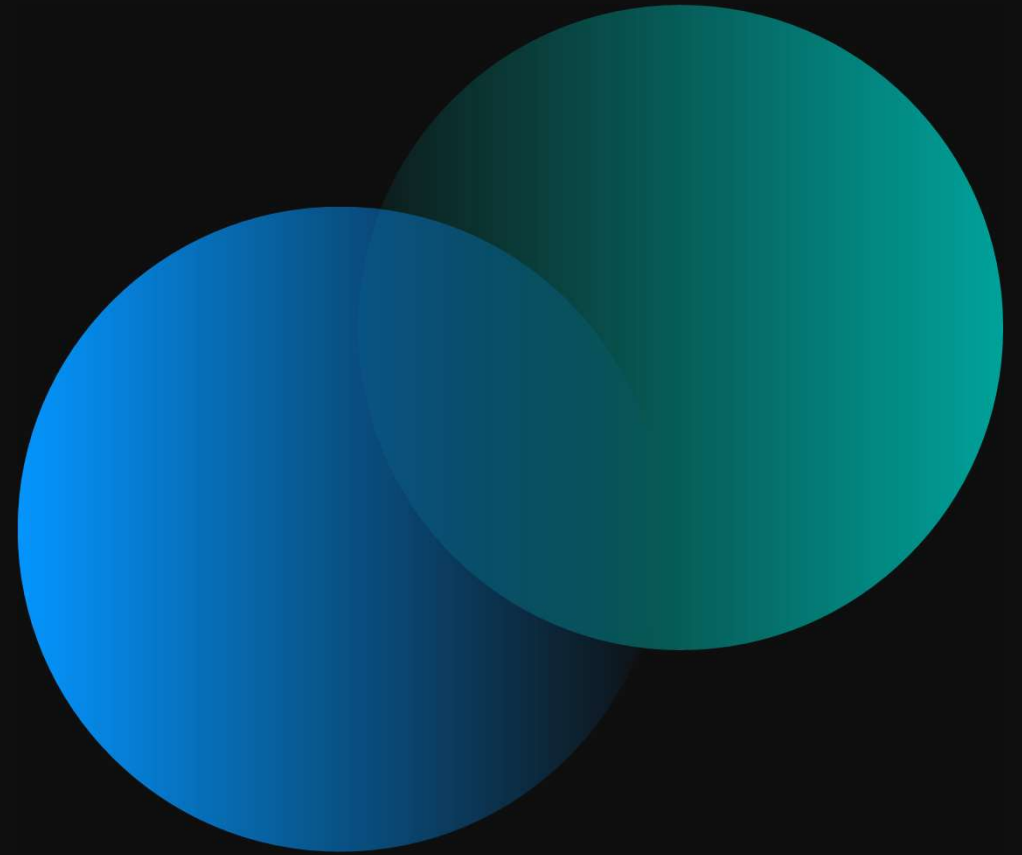
USER MANAGEMENT					
This page allows you to view and manage all users of your applications. Add a new user with the + new button at the top of the list.					
+ ADD NEW USER DELETE IMPORT					
🔍 idaas.ne					
☐	User Name	Display Name	Email	Unlocked/Locked	Actions
☐	ragots96	Scholastique RAGOT	scholastique.ragot_96@idaas.net	🔒	 
☐	pierronh92	Hildebert PIERRON	hildebert.pierron_92@idaas.net	🔒	 
☐	pasquiea95	Ancelin PASQUIER	ancelin.pasquier_95@idaas.net	🔒	 
☐	marchala100	Ameliane MARCHAL	ameliane.marchal_100@idaas.net	🔒	 
☐	marcelr98	Robert MARCEL	robert.marcel_98@idaas.net	🔒	 
☐	goupiln97	Nicolas GOUPIL	nicolas.goupil_97@idaas.net	🔒	 
☐	boutetm99	Marius BOUTET	marius.boutet_99@idaas.net	🔒	 
☐	bellecc91	Claire BELLEC	claire.bellec_91@idaas.net	🔒	 
Items per page: 25 1 - 8 of 8 < >					

Auto-inscription utilisateur



- Formulaire d'inscription entièrement **personnalisable**
- Conformité à la politique de mot de passe **en ligne**
- **Captcha** pour empêcher la création automatisée d'utilisateurs
- Inscription auprès des **fournisseurs d'identifiants sociaux** activés
- **Activation** de compte sécurisée pour imposer l'utilisation de **MFA** ou **2FA**

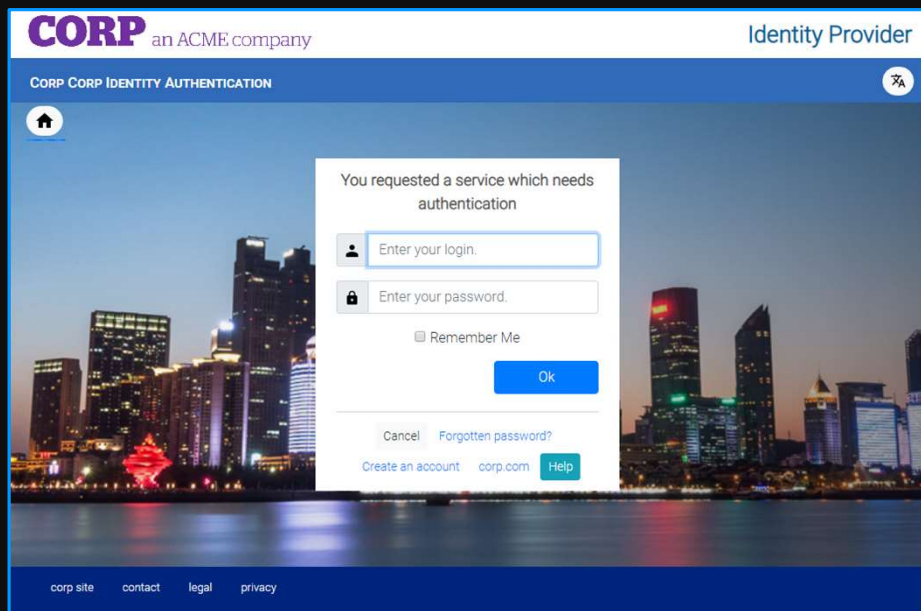
3.4 Accès utilisateur & SSO



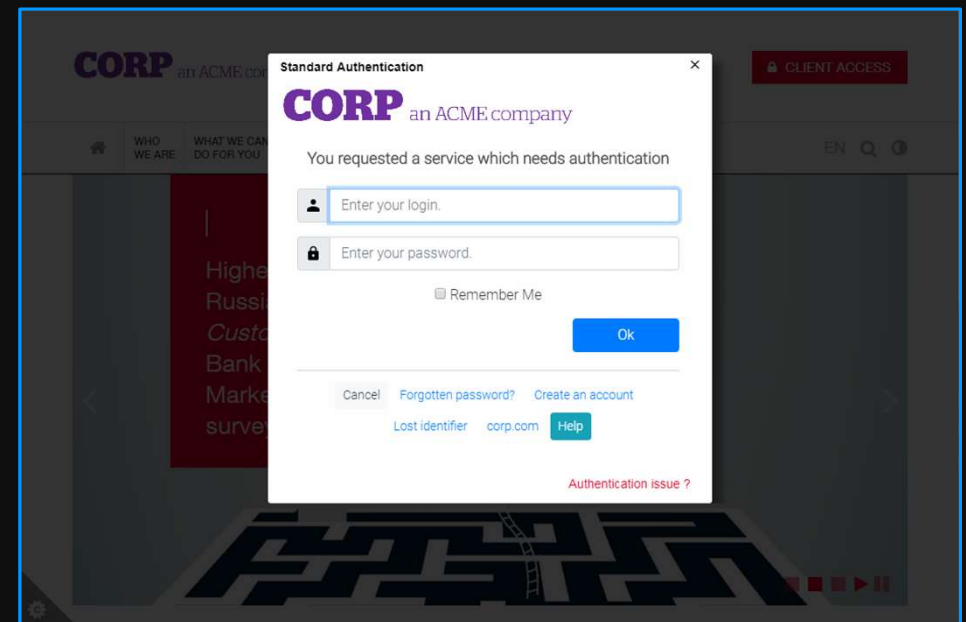
Portail d'accès Web



Un **point** d'accès **central** pour toutes les applications avec **Single Sign-On...**



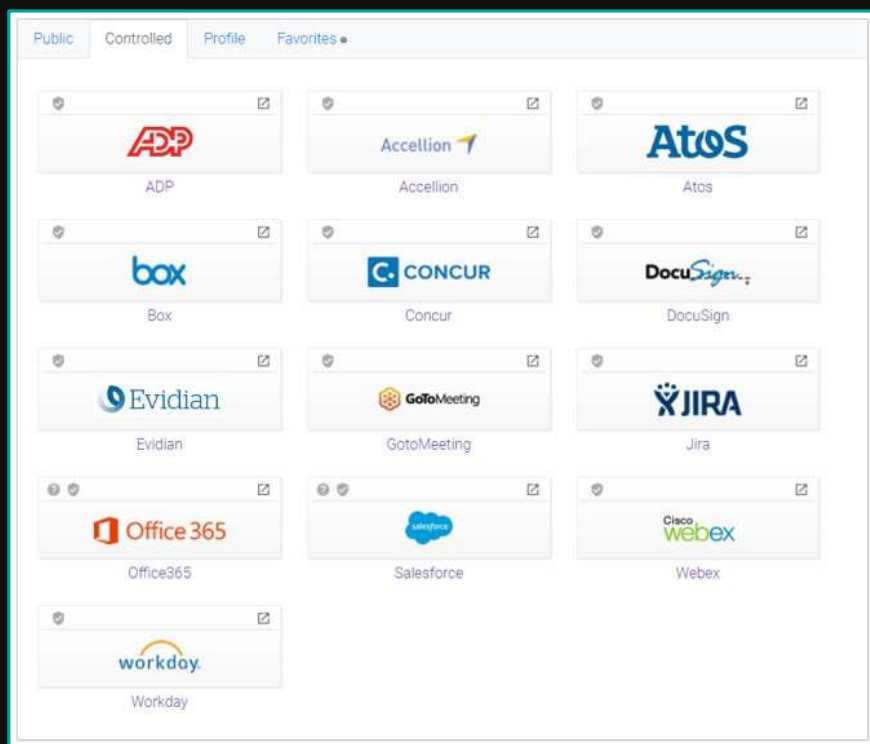
En tant que portail d'accès entièrement **personnalisable**



et/ou **intégré** à vos pages web existantes

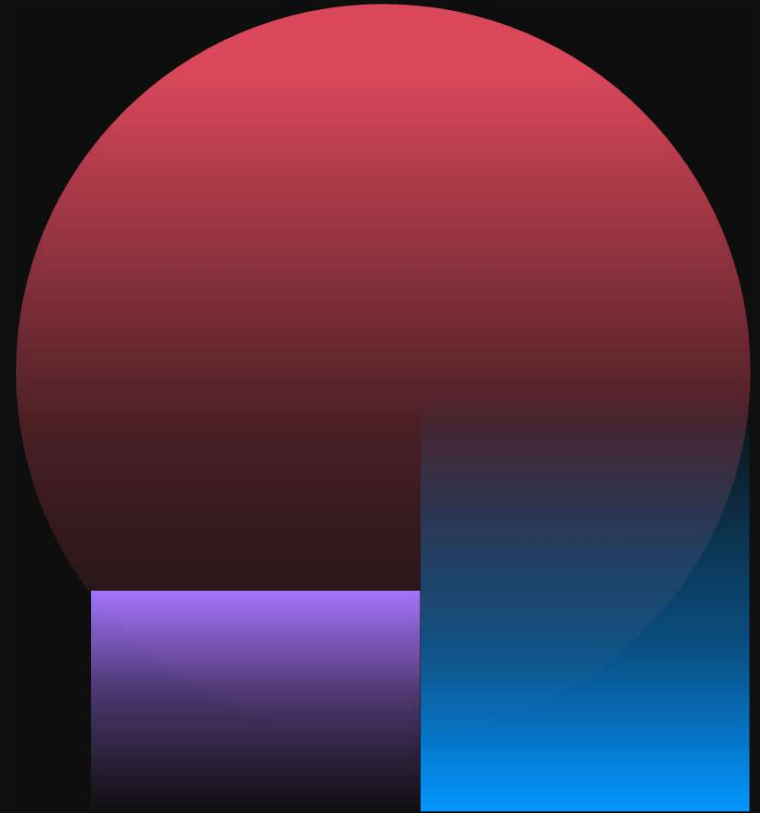
Toutes les applications sur une seule page

Authentifiez-vous une fois et accédez aux applications



- Gestion des accès : seuls les utilisateurs sélectionnés peuvent accéder à une application
- Niveau d'authentification minimal par utilisateur
- Niveau d'authentification minimal par application : les utilisateurs doivent se ré-authentifier si leur session n'est pas suffisamment sécurisée

3.5 Analytics

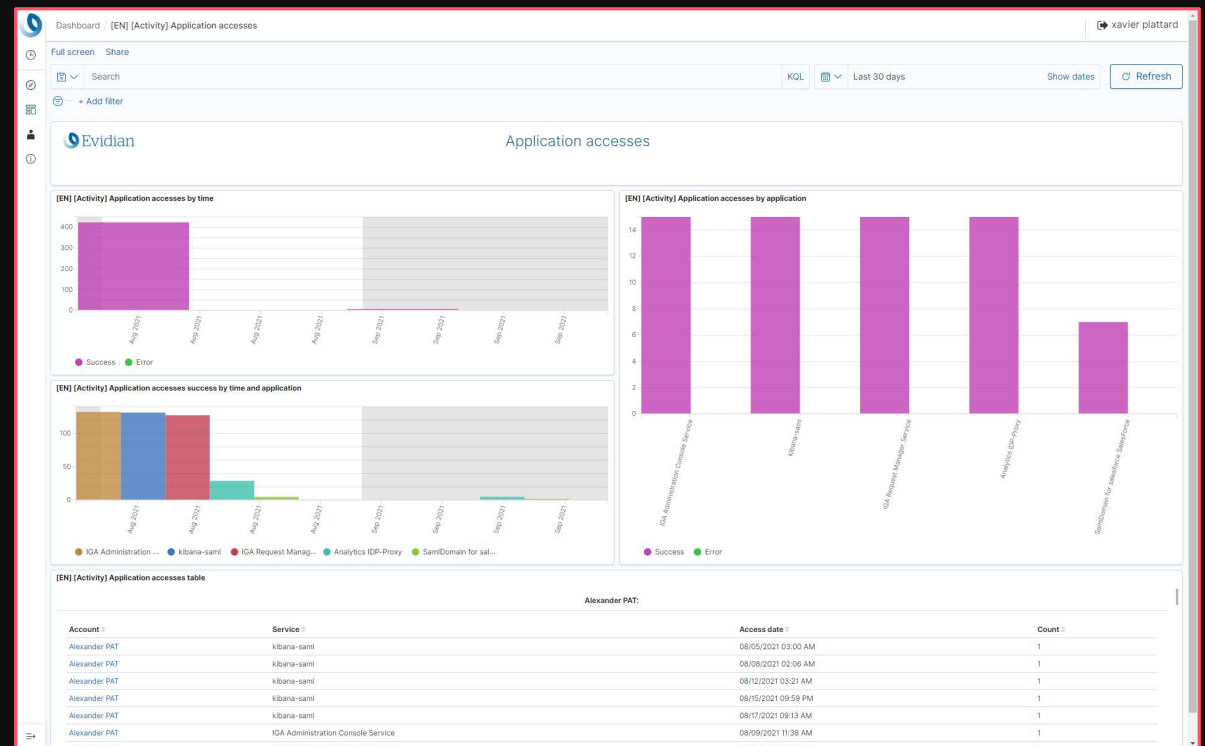


Portail Analytics

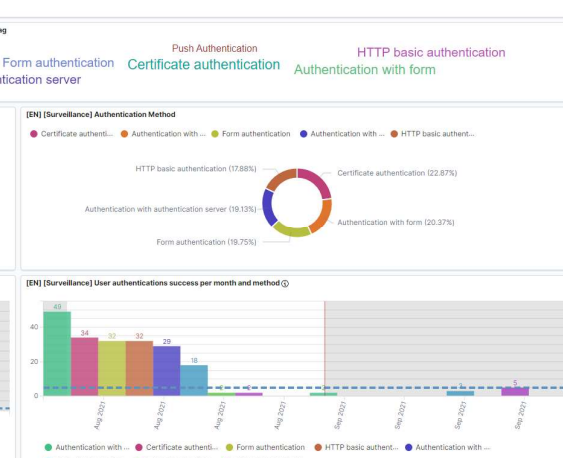
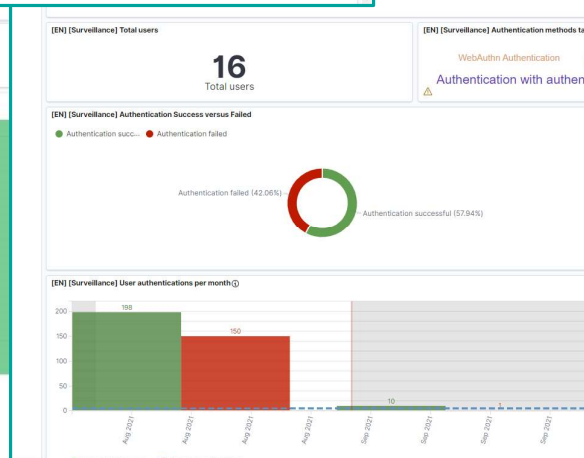
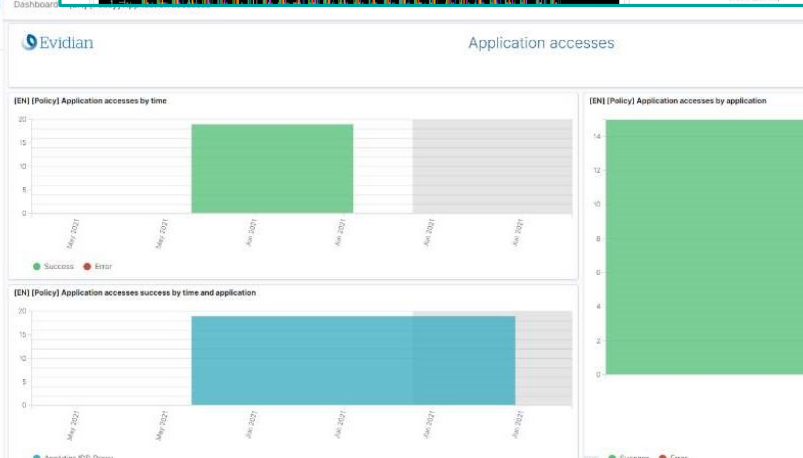
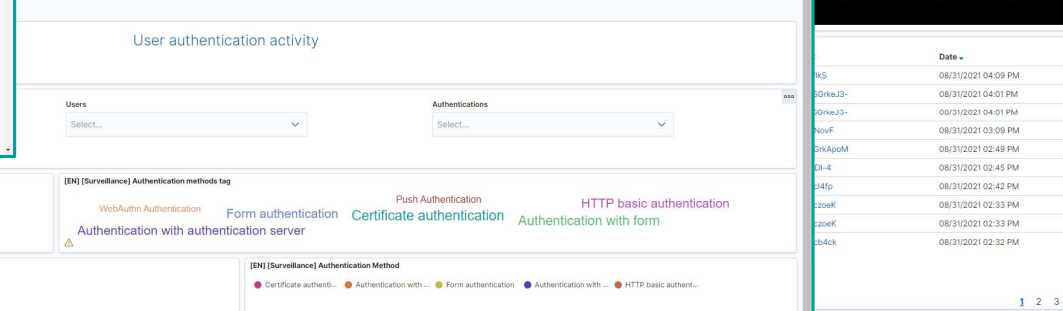
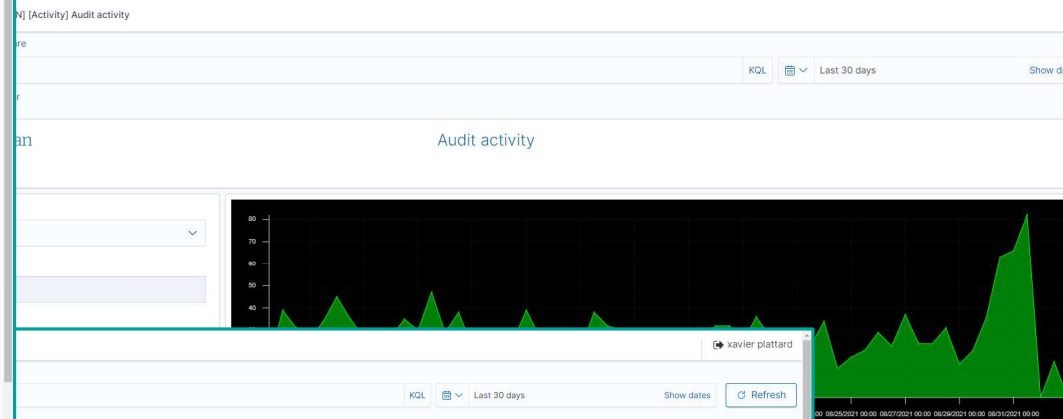
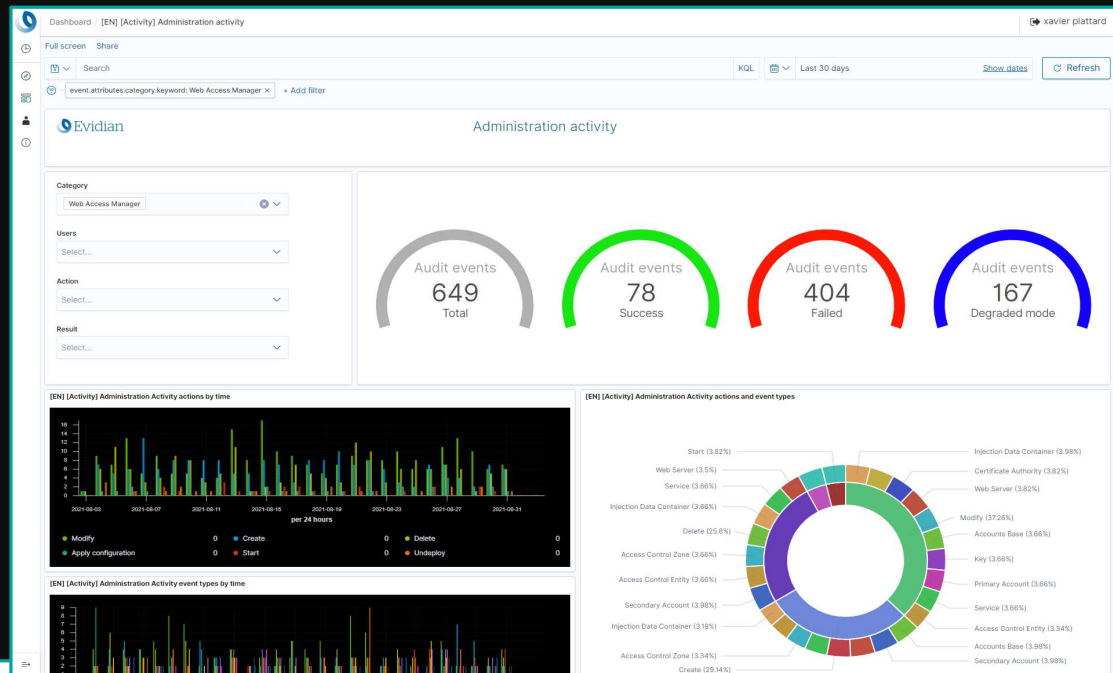


De beaux **tableaux de bord** pour surveiller l'activité des utilisateurs

- Tableaux de bord **prédéfinis** : activités d'administration, activités d'authentification, accès aux applications, ...
- **Filtrage** et **exportation** de données simplifiés.
- Capacité d'**exploration** : jusqu'à l'événement **individuel**

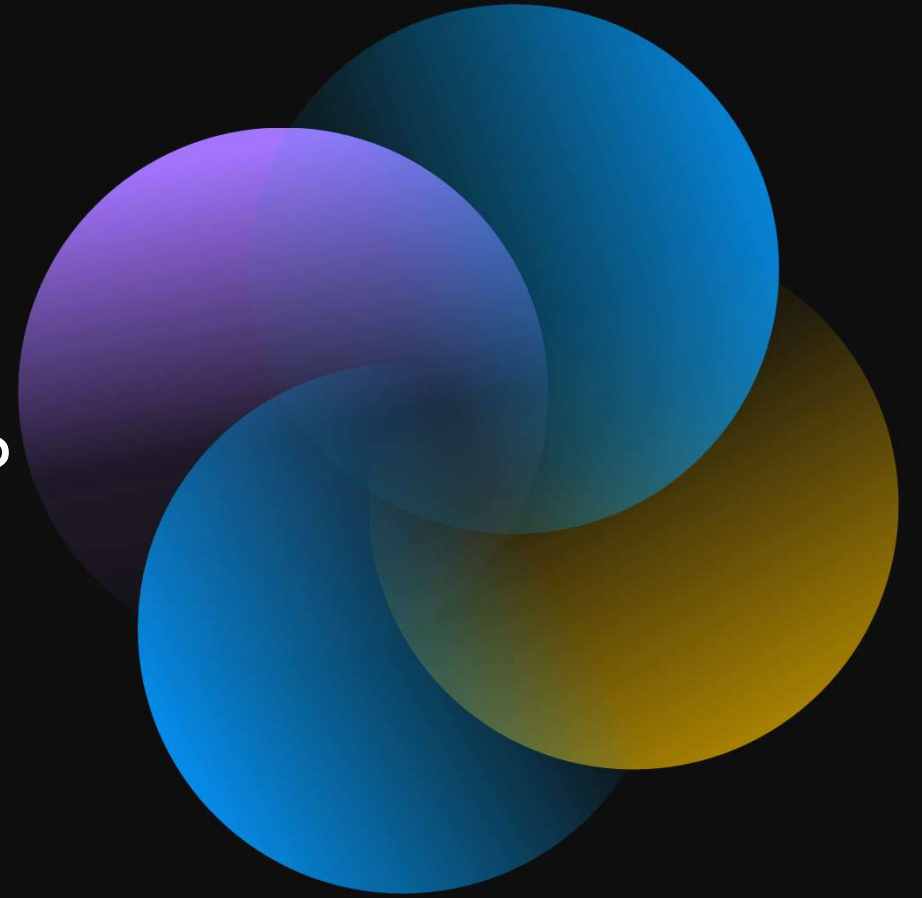


Tableaux de bord - Analytics



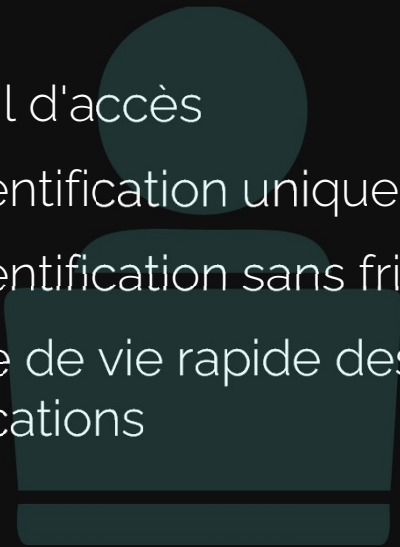
AtoS

4. Qu'y a-t-il dans l'accord ?

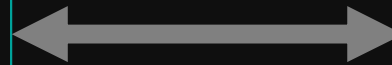


Confort d'utilisation

- Portail d'accès
- Authentification unique
- Authentification sans friction
- Durée de vie rapide des applications

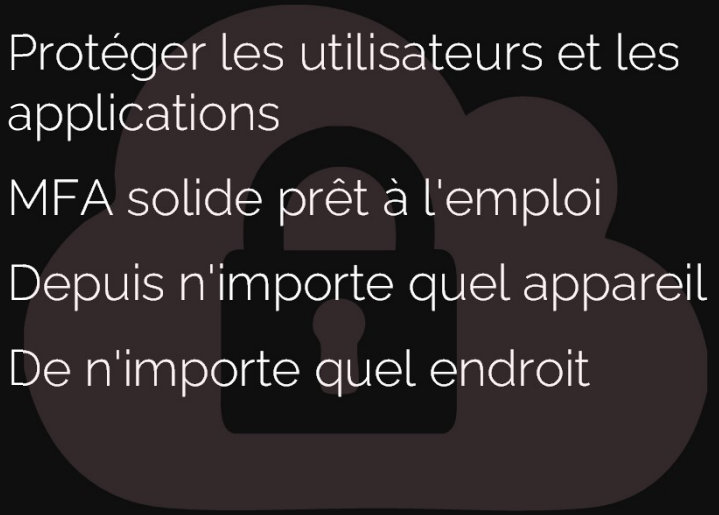


between



Sécurité

- Protéger les utilisateurs et les applications
- MFA solide prêt à l'emploi
- Depuis n'importe quel appareil
- De n'importe quel endroit



Prêt à l'emploi



Méthodes **MFA solides** prêtes à l'emploi
inc. FIDO, poussée mobile, OTP

Modèles d'applications pour vivre
rapidement

Prise en charge des applications **mobiles natives**
Serveur d'autorisation OAuth

Importation des **utilisateurs** extrait
de répertoire ou API SCIM

Portail d'accès et **SSO** SDK entièrement
personnalisable et d'intégration

**Identité complète en tant
que service**

- Intégration rapide
- Évolutivité Approche
- Evergreen



Confiance



Deux **exigences**

- se conformer à la **réglementation**
- consommateurs exigeant plus de respect de leur **vie privée**

Laissez l'utilisateur **contrôler**

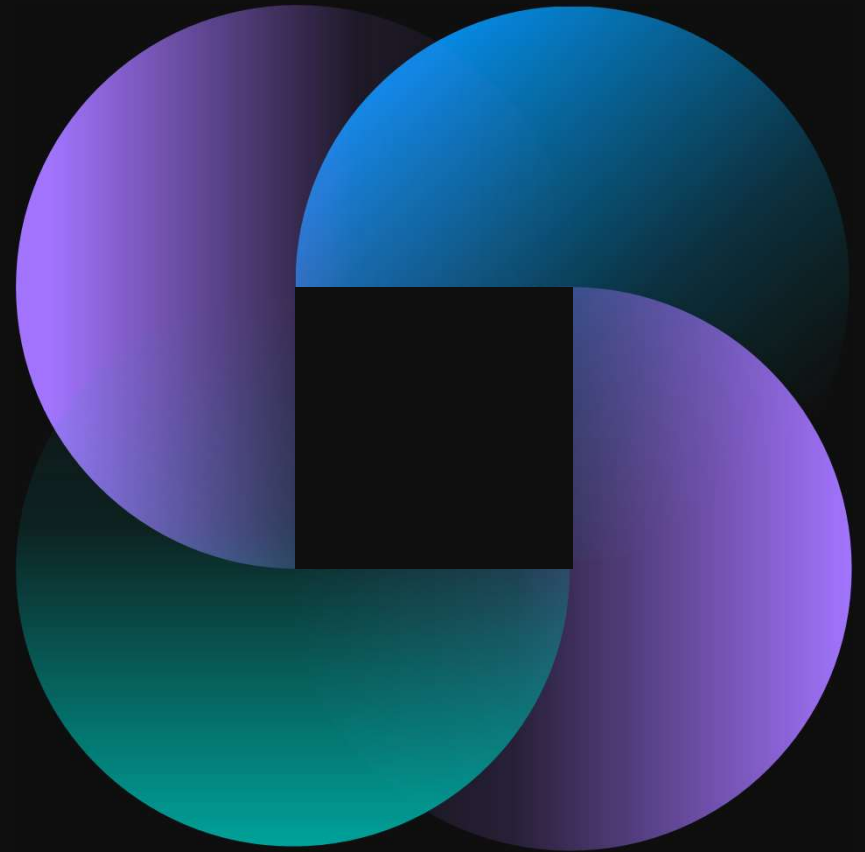
- **tableau de bord** personnel
- accéder et corriger ses **données**

Gestion intégrée des **consentements**

- au moment de l'inscription
- par les clients post factum depuis leur portail personnel

Fonction de rapport d'accès malveillant **en un clic**

Q & R



AtoS

Merci

Pour plus d'informations, veuillez contacter:

M+ 33 6 87 73 53 70
franck.laloum@atos.net

Atos, the Atos logo, Atos | Syntel are registered trademarks of the Atos group.
August 2021. © 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.

© Atos - For internal use

The Atos logo is displayed in a bold, blue, sans-serif font. The letter 'o' is stylized with a horizontal line through its center.