

Excellence en matière de Cybersécurité



Présentation Aegis Technologies

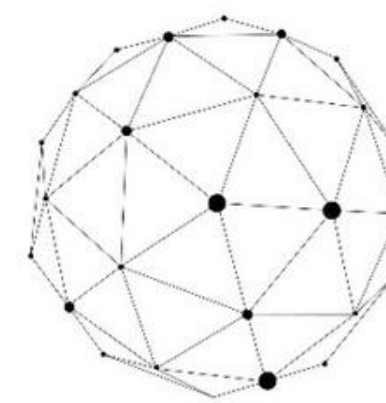
Structure d'entreprise:

- Détenu par AdamantWare, une société de solutions techniques, et appartient à ALCRAL A.G., une société de gestion d'actifs et d'investissement.
- ALCRAL A.G. a acquis les brevets et la plateforme de Swivel Secure Limited, avec une présence dans plus de 50 pays.



ALCRAL AG
— ASSET MANAGEMENT —

ADAMANTWARE
Corner-stone Technology





AEGIS
Shield One



AEGIS AUTHENTICATION
TECHNOLOGIES

Solution Aegis Technologies : Shield One



Mission et valeurs :

- Fournir les meilleures solutions d'authentification, en donnant la priorité à la qualité des produits et à l'innovation.
- Nos valeurs : excellence, qualité de produit immuable, innovation continue et sécurité robuste.
- Évolutif, flexible et s'intègre parfaitement à vos systèmes existants.



Compétence:

- Solution spécialisée dans les solutions d'authentification robustes pour la protection des actifs numériques.
- Plus d'une décennie d'expérience dans l'industrie dans la conception et le support de solutions d'authentification.



Sécurité élevée :

- Protégez et sécurisez les processus commerciaux des clients, l'accès aux applications et les données confidentielles sur les systèmes de l'entreprise. Garantisiez la sécurité tout au long du cycle de vie de l'entreprise.



Nos solutions

- **Technologie d'authentification Unique (SSO)** : Office 365, Salesforce, SAP, Azure, fédération ADFS et autres
- **Distinction par groupe** : Parties prenantes, Salariés, Fournisseurs et/ou Clients
- **Adaptable à tous les secteurs verticaux**
- **Intégration avec des centaines d'applications**
- **Authentification unique (SSO) pour les postes de travail à distance Windows**
- **Accessibilité pour les terminaux Linux dans le Cloud**
- **Provisionnement des informations d'identification pour accéder aux applications dépourvues d'intégration SSO**

Nos Solutions

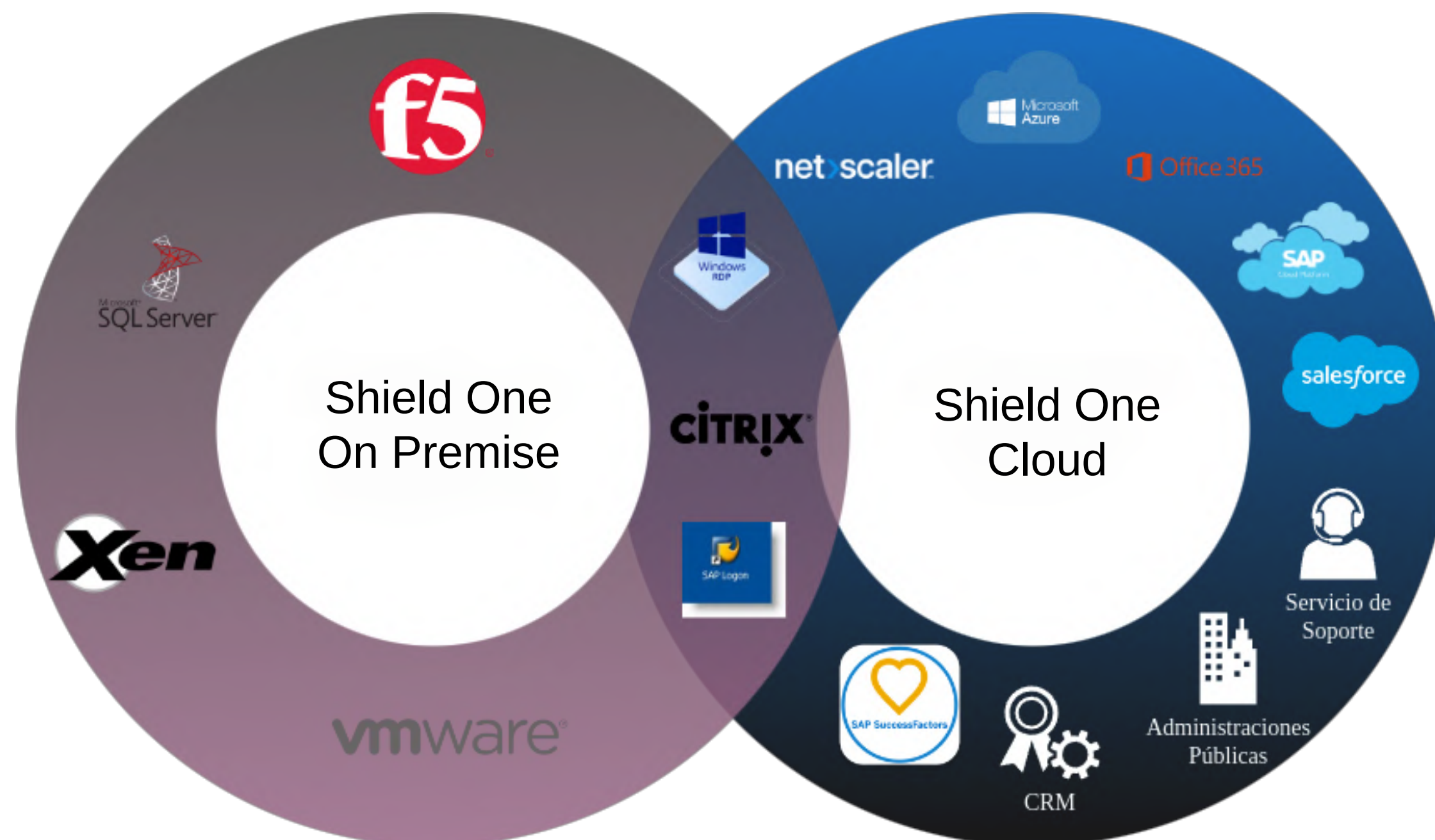
Modèle d'affaires

Modèle de livraison

■ **On Premise**

■ **Hybride**

■ **Cloud**



Shield One

- Intégrations
- Service d'assistance
- Entretien
- Solutions sur mesure



Licence

- Par utilisateur
- Par an



Clientèle

- Secteur Public
- Secteur Privé
- Services Financiers



Canal de vente

- Les Opérateurs
- Intégrateurs

Interface Aegis



AEGIS AUTHENTICATION
TECHNOLOGIES

Connexion à
Shield One^{MT}



Nom d'utilisateur

Soumettre Clair

© 2024 Aegis Technologies. All rights reserved.
Aegis Authentication Solutions

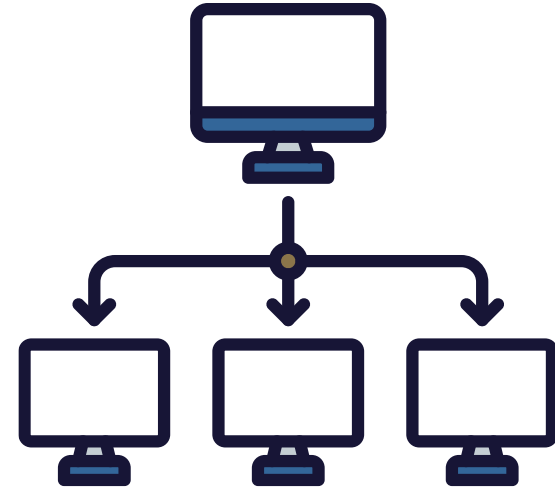
Version: 4.2.0.6601

Connectivité

WEB



LAN



VPN



VDI





Nos Protocoles et Intégrations



- **Protocoles et Intégrations Standard**

- SAML
- ADFS
- RADIUS
- Nos propres API
- OpenID
- Oauth2

- **Intégrations non Standard**

- Applications Thick Client
- Ressources sans SSO
- Oauth2 personnalisable
- Développement
- Authentification Adaptative

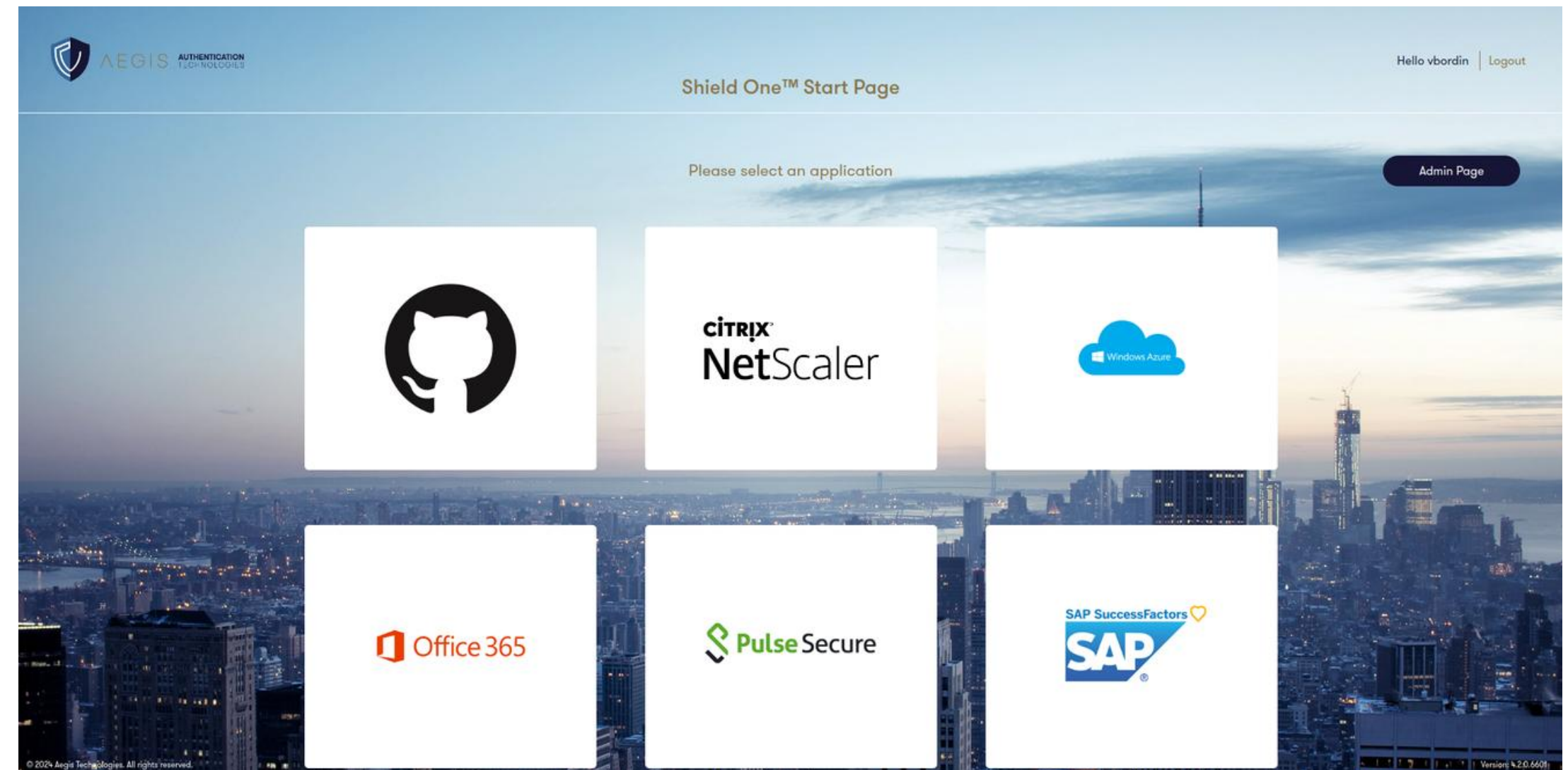


Authentication Unique (Single Sign-On)

Authentication Unique - SSO

Portail d'accès aux applications unifié :

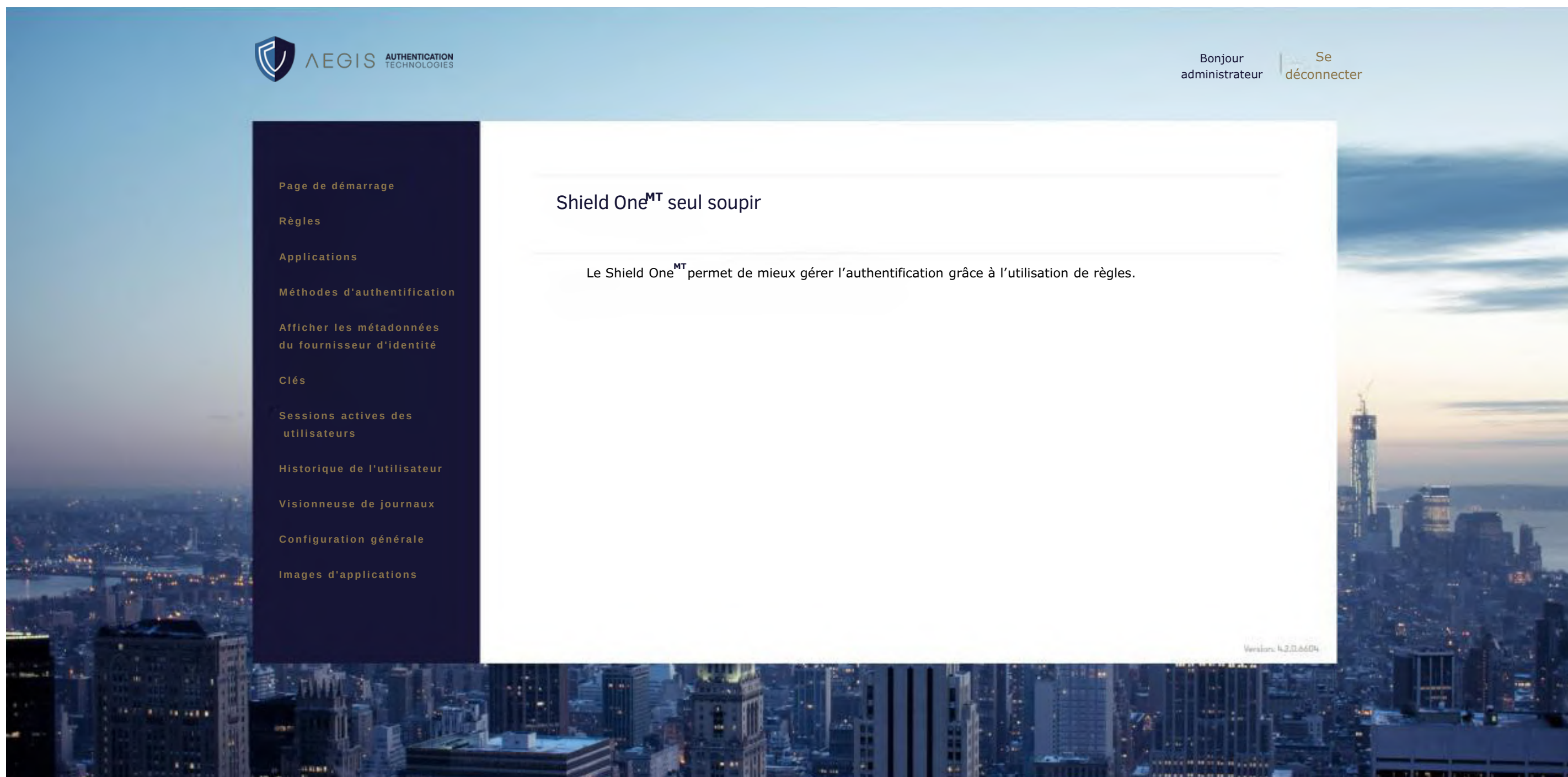
- **Gestion Centralisée** : Contrôle des droits d'accès et autorisations des utilisateurs,
- **Autonomiser les Administrateurs** (gestion efficace),
- **Intégration transparente** avec les applications dans plusieurs environnements.
- **Interface Ergonomique** (conception intuitive, navigation facile et variété d'applications à partir d'une seule interface).



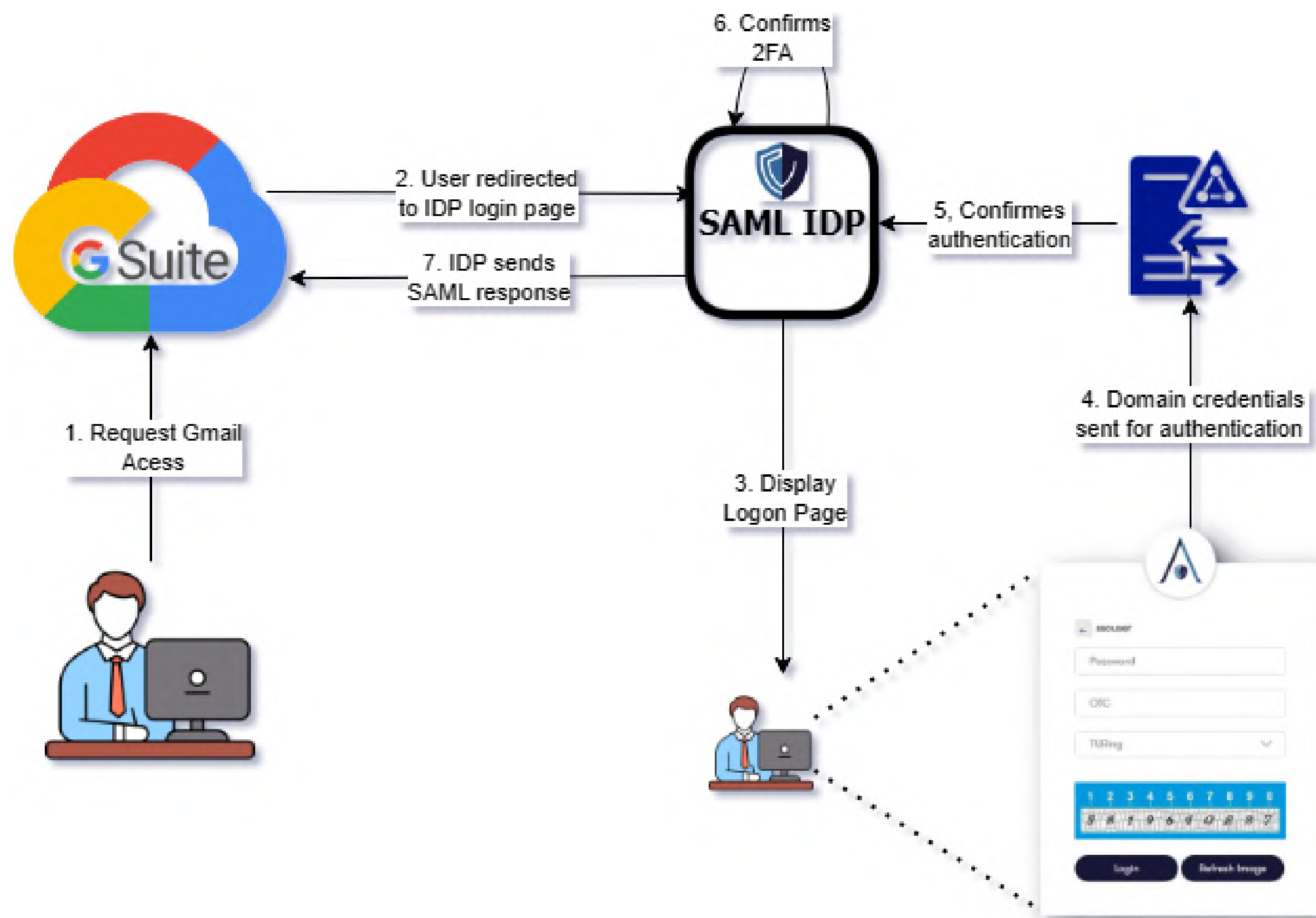


AEGIS AUTHENTICATION
TECHNOLOGIES

Aperçu du Shield One^{MT} Single Sigh-On



CAS D'UTILISATION SSO

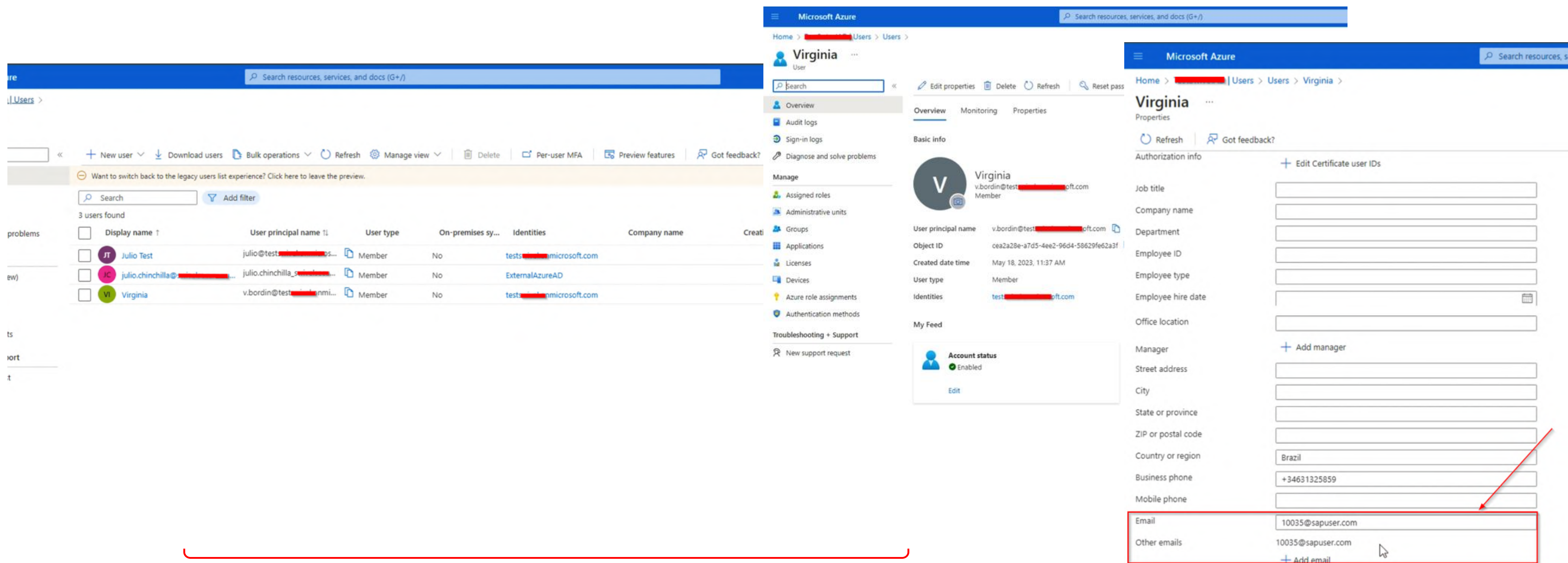


◦ Nous illustrons l'intégration seamless de notre portail **SSO** avec **G-Suite** à l'aide de **SAML**, démontrant ici le cadre de sécurité **robuste, transparent et sécurisé**.

Le portail SSO offre un accès sécurisé en tirant parti de SAML, en s'intégrant à l'infrastructure existante comme Active Directory et les mécanismes 2FA.

SAP SSO

Démo de l'authentification SSO SAP



The screenshot displays the Microsoft Azure portal interface, specifically the 'Users' section. On the left, a list of users is shown, including 'Julio Test', 'julio.chinchilla@...', and 'Virginia'. The 'Virginia' user is selected, and the right pane shows the 'Properties' tab. The 'Basic info' section displays the user's profile, including the user principal name 'v.bordin@test...oft.com', object ID, and creation date. The 'Authorization info' section shows the user's job title, company name, department, employee ID, employee type, employee hire date, office location, manager, street address, city, state or province, ZIP or postal code, country or region (Brazil), business phone (+34631325859), and mobile phone. The 'Email' field is highlighted with a red box, showing the email address '10035@sapuser.com'. A red arrow points to the 'Add email' button below the email field.

Display name	User principal name	User type	On-premises sy...	Identities	Company name
Julio Test	julio@test...	Member	No	tests...microsoft.com	
julio.chinchilla@...	julio.chinchilla_...	Member	No	ExternalAzureAD	
Virginia	v.bordin@test...nmi...	Member	No	tests...microsoft.com	

Basic info

Virginia
v.bordin@test...oft.com
Member

User principal name: v.bordin@test...oft.com
Object ID: cea2a28e-a7d5-4ee2-96d4-58629fe62a3f
Created date time: May 18, 2023, 11:37 AM
User type: Member
Identities: test...oft.com

Authorization info

Job title:
Company name:
Department:
Employee ID:
Employee type:
Employee hire date:
Office location:
Manager:
Street address:
City:
State or province:
ZIP or postal code:
Country or region: Brazil
Business phone: +34631325859
Mobile phone:
Email: 10035@sapuser.com
Other emails: 10035@sapuser.com
+ Add email

Processus qui permet aux utilisateurs Azure de se connecter à leurs postes de travail et d'accéder de manière transparente à SAP Login à l'aide de leurs informations d'identification Azure AD. L'utilisateur est associé à l'ID 10035 dans SAP.

SAP SSO

Démo de l'authentification SSO SAP

AEGIS AUTHENTICATION TECHNOLOGIES

Status

Log Viewer

Server

Policy

Logging

Messaging

Database

Mode

Repository

RADIUS

Migration

Appliance

OATH

Config Sync

Reporting

User Administration

Save Configuration

Upload Email Images

Administration Guide

Logout

AEGIS Shield One™ 2024

Aegis Primary Appliance

User Administration ?

Max No. Displayed Users: 500 (3 users in this repository)

Repository: AzureUsers

Search: username Contains

View: Attributes

Users per page: 50

State: All

Members of group: ---ANY---

Search

Reset

Purge

Undelete

Add User

Import...

User Sync

Stop User Sync

Sync Count

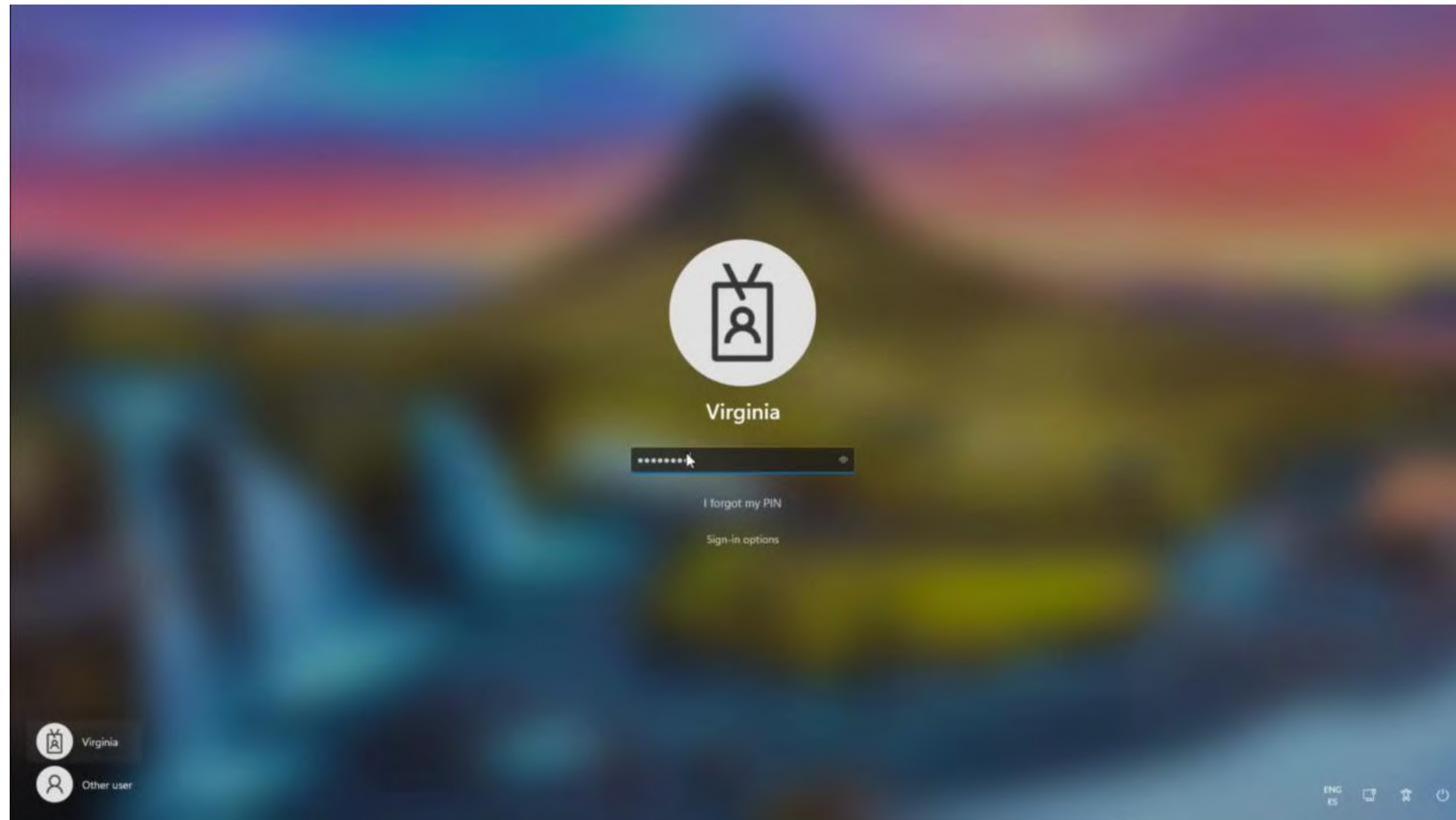
Remove All Palmprints

Username	Base_SAP_Account	altusername	email	familyname	fingerprint	givenname	other_mail	phone	platformandpushid	prc
julio.chinchilla@swivels.eu chinchilla			julio.chinchilla_swivels@swivels.onmicrosoft.com							
julio test			julio@tests@swivels.onmicrosoft.com							
virginia	10035		v.bordin@tests@swivels.onmicrosoft.com				10035@sapuser.com	+34631325859		

Exemple de synchronisation parfaite des utilisateurs avec le serveur Shield One directement à partir d'Azure AD. Le **champ Base_SAP_Account** affiche l'ID SAP de l'utilisateur, qui est mappé à partir d'Azure AD. De plus, d'autres attributs d'Azure AD sont synchronisés avec succès grâce au serveur Shield One, garantissant ainsi un profil utilisateur complet et unifié.

SAP SSO

Démo de l'authentification SSO SAP



Ici, l'utilisateur accède au poste de travail à l'aide des informations d'identification Azure AD et sélectionne SAP Logon pour lancer le processus de connexion et se connecte de manière transparente à SAP Logon avec l'expérience SSO.



MFA

MFA

Présentation de notre MFA et de notre ePinsafe® breveté :

Notre **ePinsafe®**, notre technologie éprouvée d'authentification multifacteur (MFA) sans jeton. Avec **plus de deux décennies** de mise en œuvre réussie.

Qu'est-ce qu'ePinsafe® ?

- ePinsafe® est notre technologie brevetée qui prend en charge divers facteurs d'authentification, notamment Image PINpad, PICpad et TURing.

Flexibilité d'intégration :

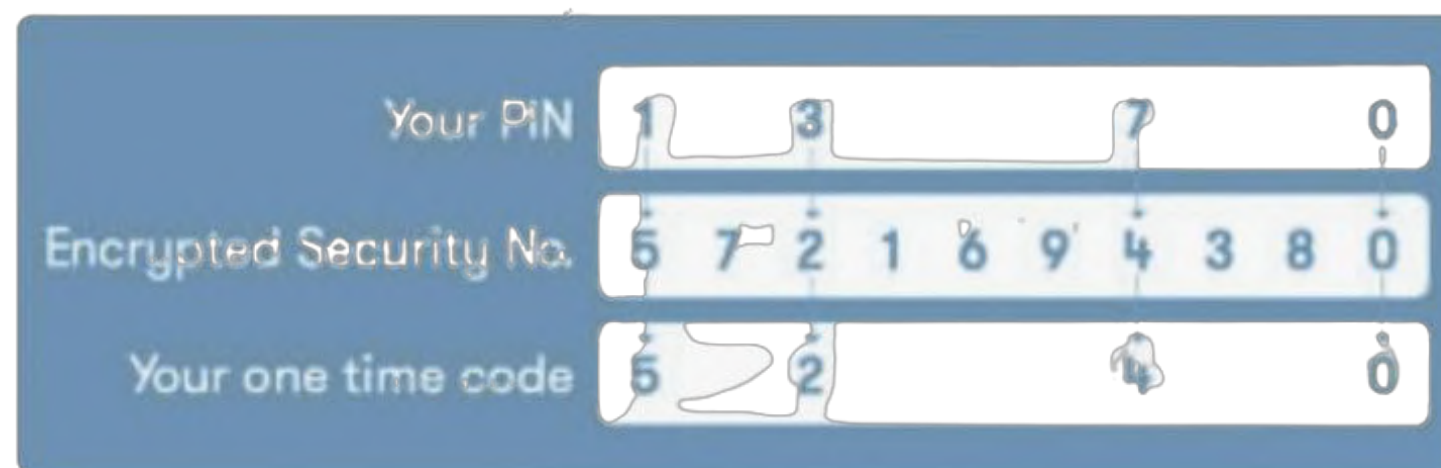
ePinsafe® s'intègre de manière transparente à divers appareils et applications, notamment :

- **Connexion Windows (accès à distance avec F5, Citrix Netscaler et Cisco VPN).**
- **Accès Web (OWA, Apache et Microsoft IIS).**

Comment fonctionne Tokenless ePinsafe® ?

Les utilisateurs se voient attribuer un numéro d'identification personnel (PIN), qu'ils ne saisissent jamais directement. 1370 dans cet exemple :

- Lors de l'authentification, les utilisateurs reçoivent une chaîne de sécurité à 10 chiffres (par exemple, 5721694380) via un affichage graphique ou un e-mail/SMS de vérification.
- En utilisant le code PIN comme indicateur de position, un code unique à usage unique (par exemple, 5240) est extrait pour une authentification sécurisée.

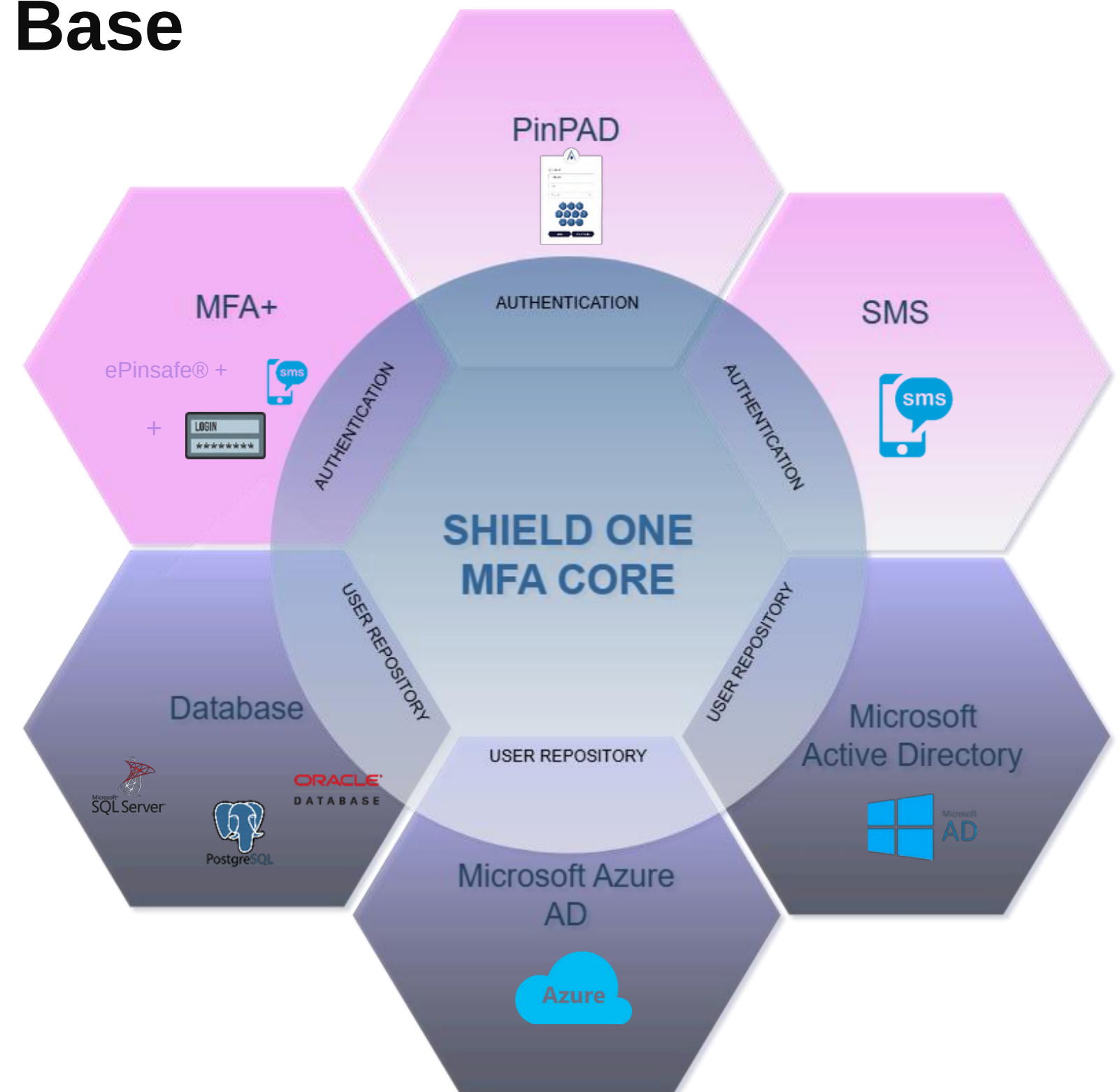
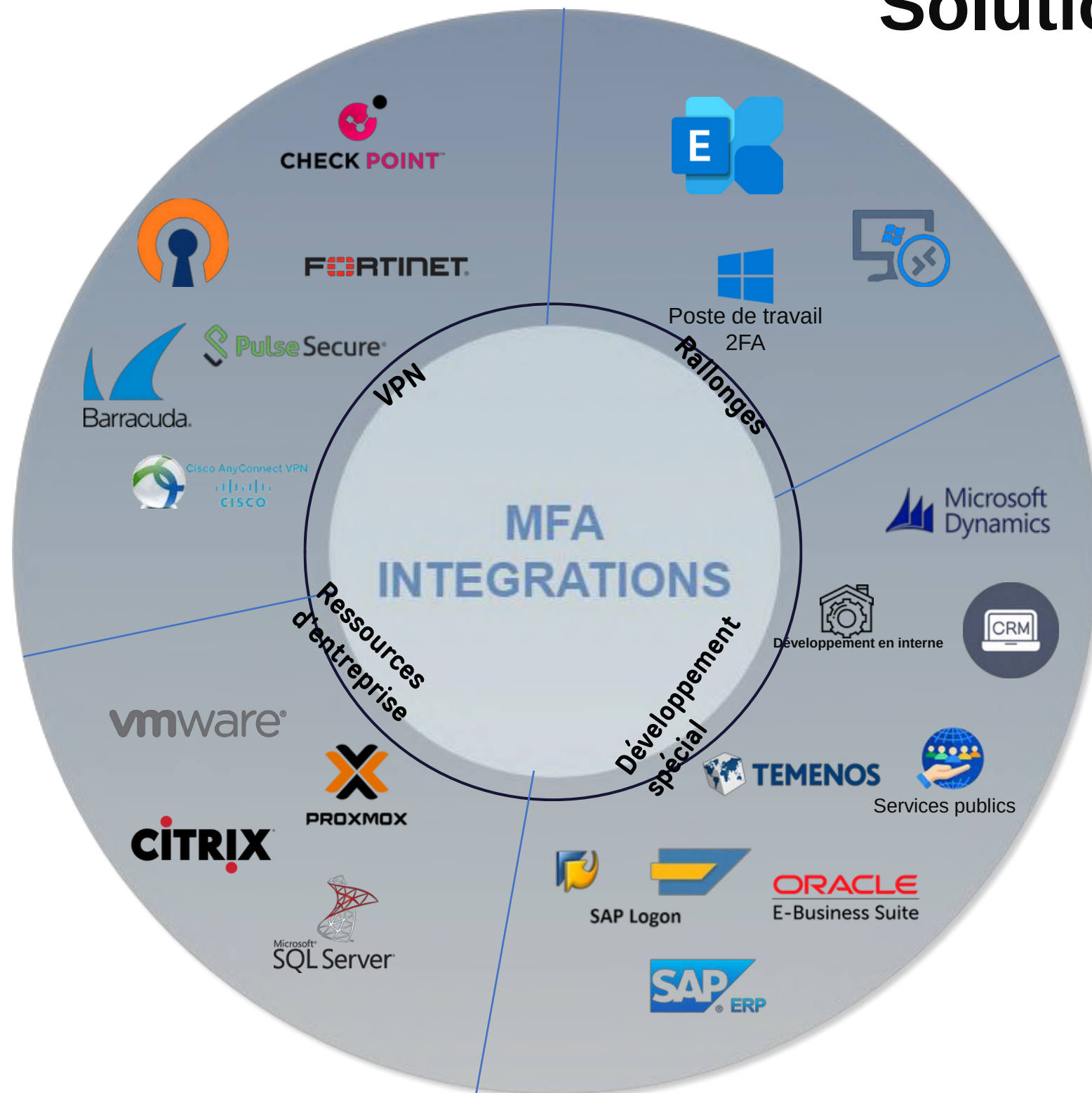




AEGIS AUTHENTICATION
TECHNOLOGIES

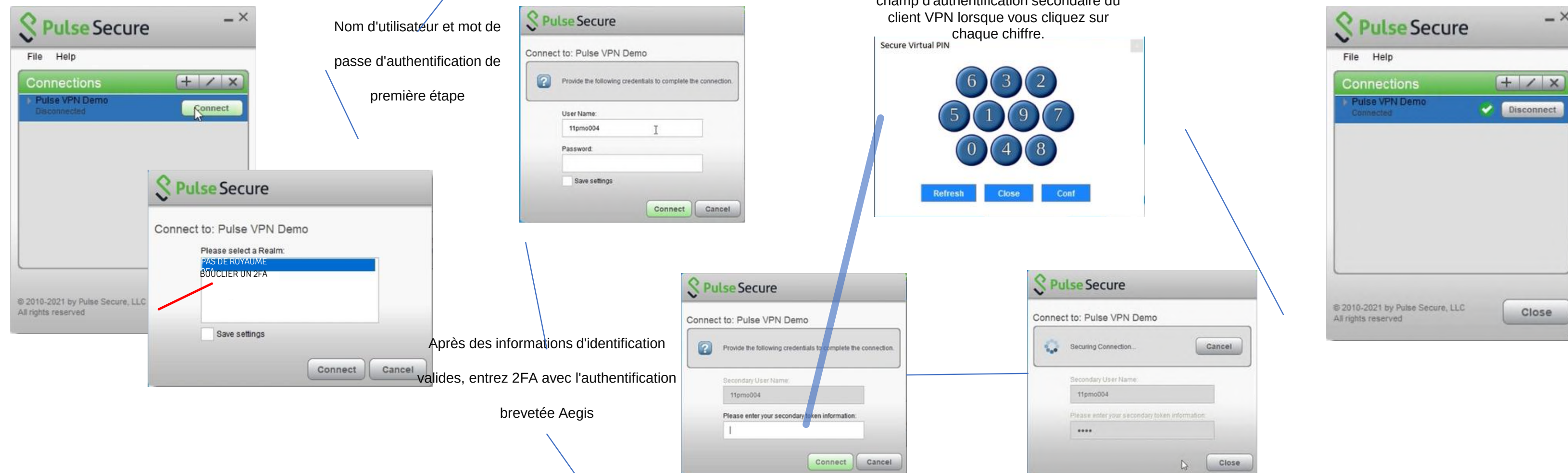
MFA

Solution de Base



CAS D'UTILISATION MFA

Solution de base MFA



La méthode **d'authentification brevetée PinPAD** sans jeton permet aux utilisateurs de saisir en toute sécurité leur code PIN via un clavier numérique virtuel pour accéder au VPN. Ajoute une couche de sécurité supplémentaire, prenant en charge divers protocoles et services d'authentification.

Exemple de flux avec le client VPN Pulse Secure.



Authentificateurs

Facteurs d'authentification

Aegis propose une large gamme de facteurs d'authentification :

- Application mobile - Shield One Mobile
- SMS
- Image
- Biométrie
- Token (Jeton) Physique

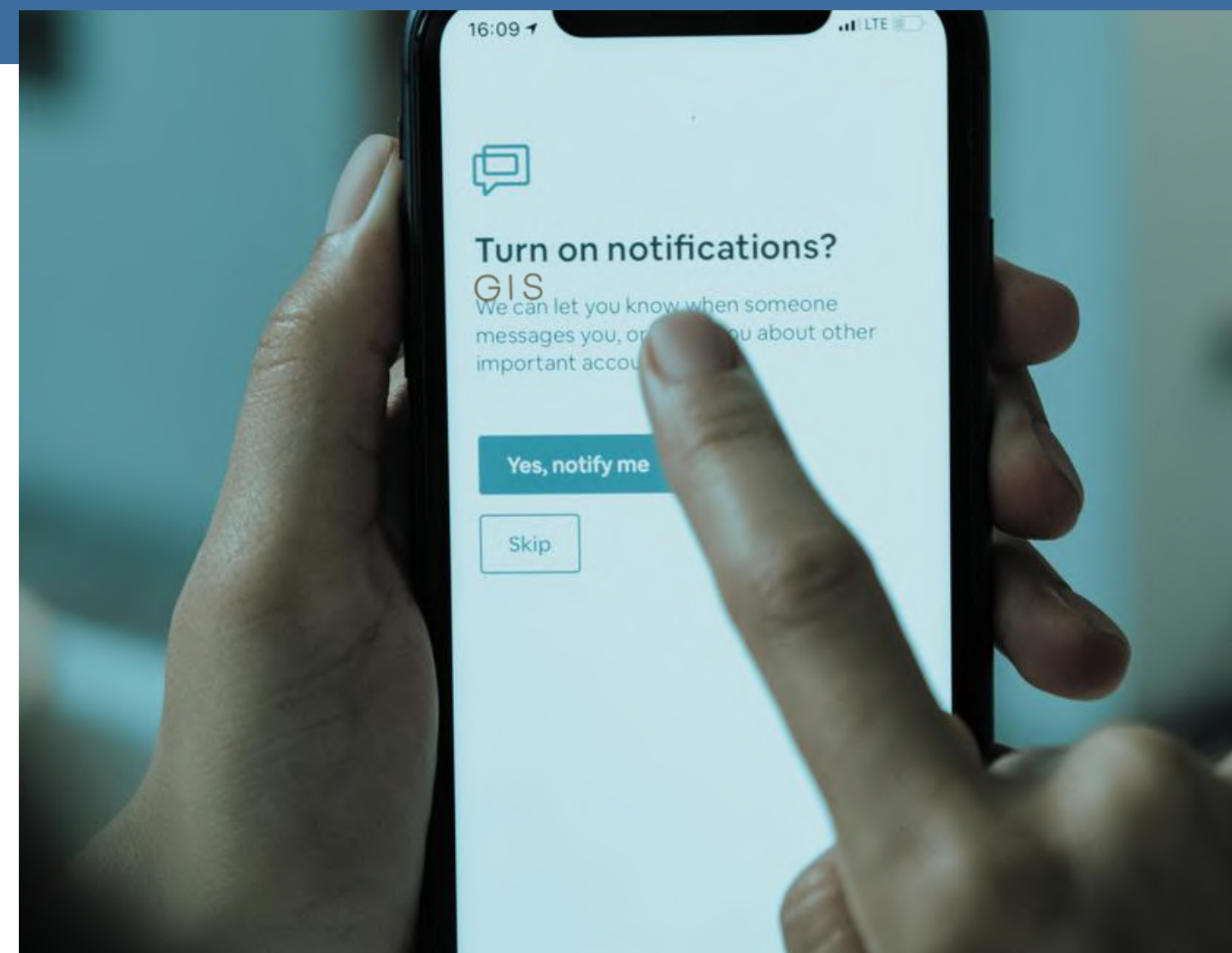
Technologie PINsafe® brevetée :

PINsafe® est la technologie brevetée qui prend en charge les facteurs d'authentification tels que Image PINpad, PICpad et TURing, tous dans la gamme de facteurs d'authentification disponibles avec Shield One.

Shield One Mobile : OTC (code à usage unique)

Chaque fois que l'application vous demande de vous authentifier, utilisez simplement l'OTC.

- 99 codes disponibles
- Peut être utilisé hors ligne.





Méthodes d'authentification

Options d'authentification étendues

- Un portefeuille de plus de 15 méthodes d'authentification différentes, y compris des **Solutions Brevetées** pour une sécurité supérieure.

Authentification Multifacteur Avancée (MFA) et Authentification à Deux Facteurs (2FA)

- Solutions flexibles MFA et 2FA.
- Workflows d'authentification adaptative adaptés aux évaluations des risques en temps réel.





Authentication Basée sur les Risques (RBA)

Authentification Basée sur les Risques

Sur la base des paramètres définis dans le système de stratégie, RBA demande le niveau d'authentification approprié pour accéder aux applications basées sur les utilisateurs, à leurs appareils et à l'application elle-même.



- Affectation à un groupe spécifique par candidature



- Emplacement d'accès : adresse IP et vitesse géographique



- Appareil utilisé pour l'accès



- Informations sur la dernière authentification : Heure / Date / Jour



- Compatibilité avec X509



- Géolocalisation - GeoIP



- Règles composites pour générer une chaîne d'évaluations des risques basées sur les technologies susmentionnées



Authentification Basée sur les Risques en Standard

Sur la base des paramètres définis dans le système de stratégie, RBA demande le niveau d'authentification approprié pour accéder aux applications basées sur les utilisateurs, à leurs appareils et à l'application elle-même.

SYSTÈME GRC

NÉCESSITE 120 POINTS

LAN	50
Known IP	50
Device	50
IP Range	50
<u>Require Authentication</u>	
U&P	10
Mobile App	60
Biometrics	20

L'utilisateur travaille au bureau et souhaite accéder au CRM pour créer une opportunité.

Ils utilisent leur ordinateur portable d'entreprise et accèdent à l'application située dans leurs locaux.

Exemple d'authentification Basée sur les Risques :

Autre cas, l'utilisateur se trouve en Asie du Sud-Est et souhaite accéder au système ERP depuis l'appareil mobile de son entreprise. Cette activité étant inhabituelle, le système d'authentification basée sur les risques peut nécessiter une vérification supplémentaire avant d'accorder l'accès.

SYSTÈME ERP NÉCESSITE 120 POINTS

LAN	0
Known IP	0
Device	50
IP Range	-100
<u>Require Authentication</u>	
U&P	dix
Mobile App	60
Biometrics	20

Flexibilité et contrôle maximum

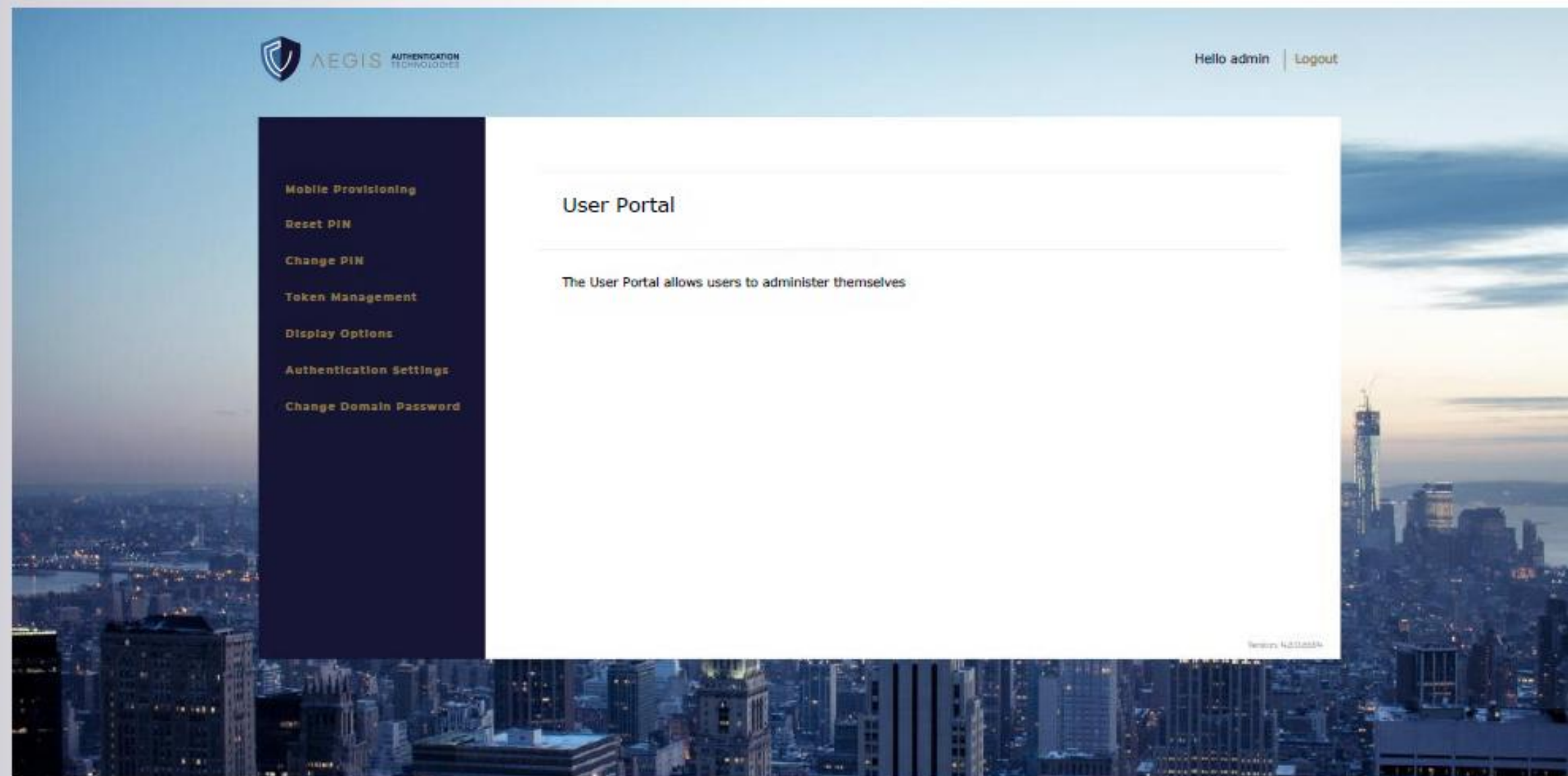
Le système de politique vous permet de créer de nouvelles règles et de les combiner avec celles existantes, dans des scénarios de plus en plus complexes.



Portail Utilisateur



User Portal Overview



- Mise à jour du mot de passe du domaine
- Gestion des Token (Jeton) Physiques (pour l'utilisation du jeton OATH, si nécessaire)
- Réinitialisation du code PIN pour l'initialisation MFA adaptative



Nos solutions

POURQUOI SHIELD ONE ?

Features Evaluation	DUO	ForgeRock	Starlink 2FA	OneLogin	MS Azure (enterprise)	Aegis Shield One
Mobile Application	✓	✓	✓	✓	✓	✓
SAML Integration	✓	✓	✓	✓	✓	✓
Oauth2 Integration	✓	✓	✓	✓	✓	✓
MFA	✓	✓	✓	✓	✓	✓
Single Sign-On Portal	✓	✓	✓	✓	✓	✓
User self service portal	✓	✓	✓	✓	✓	✓
Integration API	✓	✓	✓	✓	✓	✓
Risk Management	✓	✓	✓	✓	✓	✓
Keychain Risk Authentication	✓	✓	✓	✓	✓	✓
Microsoft Authentication with offline support	✓	✗	✗	✗	✗	✓
Web based SAP Logon authentication	✗	✗	✗	✗	✗	✓
SAP MFA	✗	✗	✗	✗	✗	✓
Patented MFA	✗	✗	✗	✗	✗	✓
AI for local application authentication	✗	✗	✗	✗	✗	✓

Aegis Shield One surpasse tous ses concurrents en offrant les fonctionnalités de sécurité les plus complètes et avancées du marché :

- **Ensemble de fonctionnalités inégalé :**
 - Au-delà des offres standards, Aegis Shield One inclut des fonctionnalités que d'autres solutions ne peuvent offrir.
- **Technologie avancée:**
 - Intègre de manière unique l'IA pour l'authentification des applications locales
 - Authentification des risques par trousseau, améliorant la sécurité grâce à une détection et une atténuation intelligentes des menaces.
- **Convivial:**
 - Portail libre-service utilisateur et capacités d'authentification unique, nous rationalisons l'accès et l'administration, améliorant à la fois l'expérience utilisateur et l'efficacité.
- **Intégration transparente:**
 - Prise en charge étendue de l'API d'intégration (garantit une intégration fluide dans vos systèmes existants).

MERCI!



www.aegisauth.com