

2 FACTOR + 2 WAY Authentication

DualShield de Deepnet est une plateforme d'authentification unifiée qui permet l'authentification forte multi-facteurs au travers de diverses applications, utilisateurs et tokens.

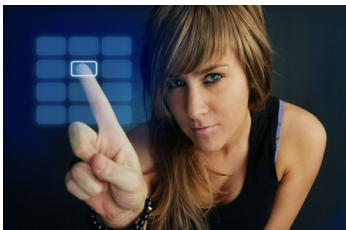


5 Star Award 2010

"A good value for the money and a nice enterprise solution."

★★★★★ SC Magazine

Introduction à DualShield



DualShield de Deepnet est une plateforme d'authentification unifiée qui permet l'authentification forte multi-facteurs au travers de diverses applications, utilisateurs et tokens.

Méthodes

- One-Time Password (OTP)
 - OTP sur portables
 - OTP sur clés USB
 - OTP sur cartes à puces
 - OTP à la demande
- Certificat Digital (PKI)
- ADN Digitale
- Biométries

Solutions

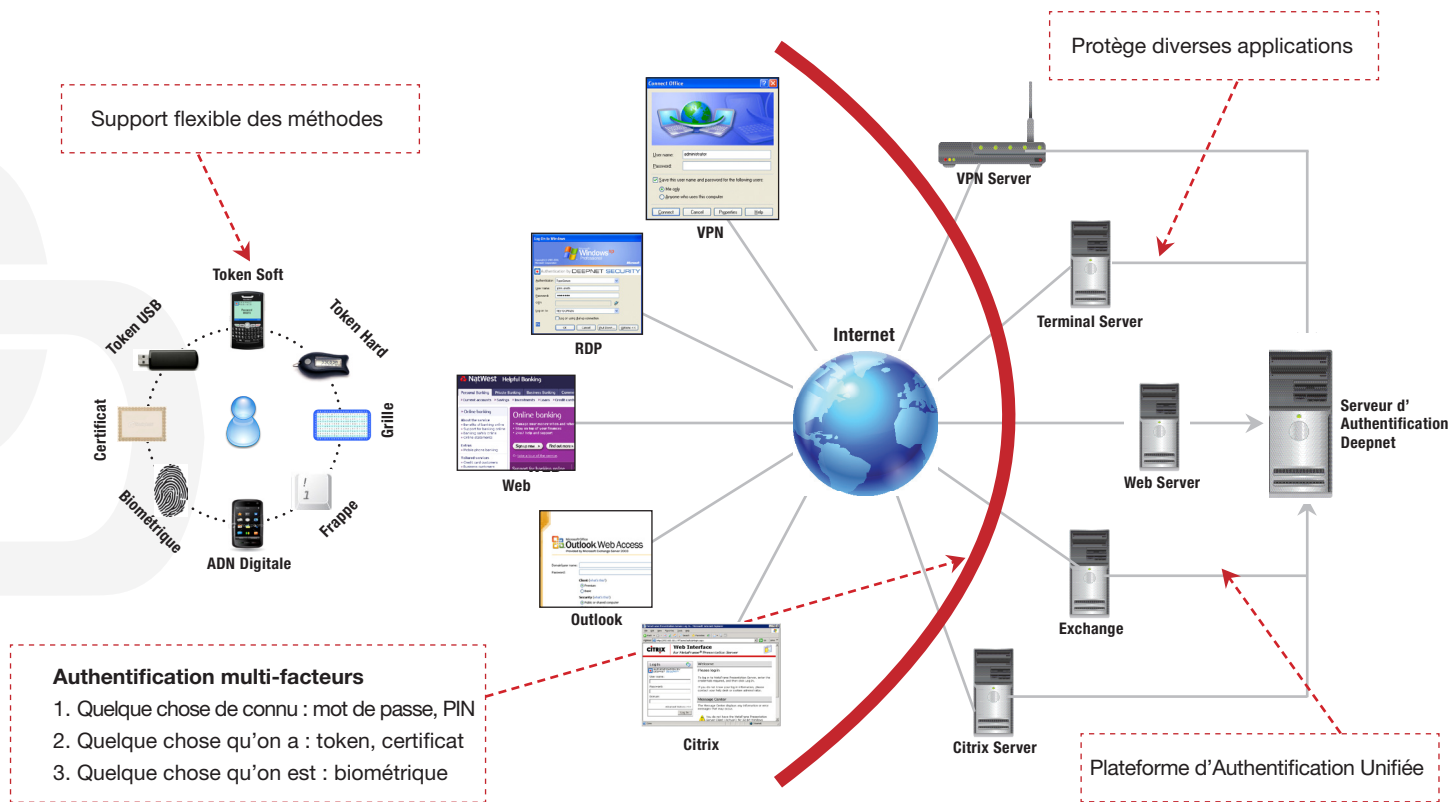
- Authentification VPN/RADIUS
- Authentification Windows/Linux
- Authentication Web
- Outlook
 - Outlook Anywhere
 - Outlook Web Access
 - Outlook Mobile Access
- Citrix
- 2X

DualShield est une solution complète pour l'authentification forte des utilisateurs très conviviale, économique et facile à intégrer dans une infrastructure existante. Le logiciel serveur supporte à la fois les serveurs Windows et Linux.

Fonctionnalités Clés

- Console de management Web
- Intégration LDAP/AD Native
- Gestion des utilisateurs centralisée
- Contrôle d'accès par rôle
- Administration par stratégie
- Rapports et audits avancés
- Support RADIUS étendu
- Portail Web self-service

Architecture de DualShield



MobileID



MobileID transforme les téléphones portables, les clés USB, les PDAs et les PCs en tokens One-Time Password (OTP) fournissant aux entreprises, aux banques, aux services en ligne et aux distributeurs un moyen économique d'apporter l'authentification forte à leurs clients, leurs partenaires et leurs employés, le tout sans déployer de tokens hardware supplémentaires.

Fonctionnalités clés

- Authentification à deux facteurs
- Authentification mutuelle
- Challenge & Response
- Signature des données
- Conformité OATH
- Deux Algorithmes (HOTP, TOTP)
- Protection par PIN
- Support multi-token

MobileID supporte

- Téléphones portables
 - Java
 - Windows Mobile
 - iPhones
 - Blackberry
- Clés USB
- PCs (Windows XP/Vista/7)



MobileID / Flash



MobileID / PC

T-Passe Mobile

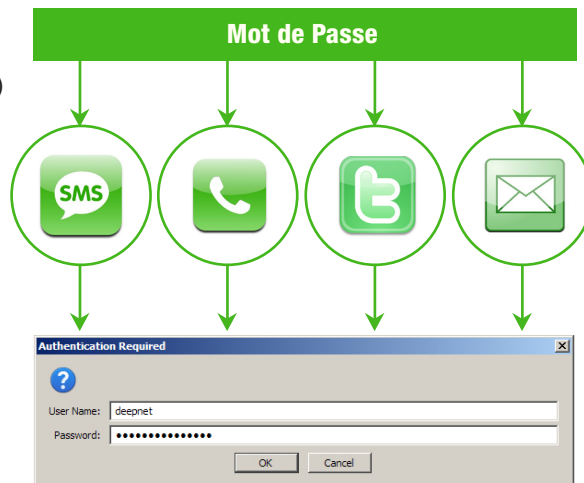
T est pour Texte, Téléphone et Twitter. T-Passe Mobile est une solution d'authentification par OTP à la demande qui délivre les mots de passe à votre téléphone par messages SMS, vocaux, twitter ou électroniques (mail).

T-Passe est une des solutions les plus conviviales et économiques d'authentification à deux facteurs. Elle ne requiert aucun déploiement de matériel ni d'installation de logiciel et donc épargne aux clients le coût de l'administration, de la formation et du support technique.



T-Pass supporte

- Texte (SMS)
- Téléphone (Vocal)
- Twitter
- Email



SafeID

SafeID est un outil de sécurité compact qui génère des one-time passwords (OTP) en appuyant simplement sur un bouton. Plusieurs modèles sont disponibles.

ONE-TIME PASSWORD



SafeID 100

Event-based. Un token “vert” à vie avec une batterie renouvelable.

- Conforme OATH (HOTP)
- Taille : 54 x 28 x 15 mm
- Batterie : remplaçable



SafeID 200

Conforme OATH TOTP, time-based. Un token de sécurité compacte et durable.

- Conforme OATH (TOTP)
- Taille : 61 x 28 x 12 mm
- Batterie : 3-5 ans



SafeID C100

Conforme OATH HOTP, event-based. De la forme d'une carte de crédit avec un affichage e-ink.

- Conforme OATH (HOTP)
- Taille : carte de crédit
- Batterie : 3 ans



SafeID C112

Conforme OATH HOTP, event-based. De la forme d'une carte de crédit avec un bloc PIN de 12 boutons.

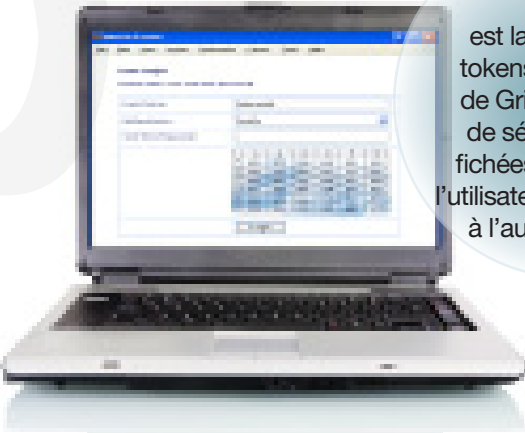
- Conforme OATH (HOTP)
- Taille : carte de crédit
- Batterie : 2 ans

GridID & GridGo

GridID est une méthode d'authentification forte, simple et efficace, basée sur des grilles de sécurité. Une grille de sécurité contient une matrice de chiffres et de lettres dans des colonnes et des lignes facilement identifiables. Ces grilles de sécurité sont typiquement imprimées sur des cartes transportables dans un porte-feuille.

Afin de réaliser l'authentification forte de l'utilisateur avec une grille de sécurité, celui-ci doit fournir un OTP généré à partir de la grille.

ACME											S/N: 10012100
	A	B	C	D	E	F	G	H	J	K	
0	w	g	2	m	1	6	8	6	7	s	0
1	v	d	2	f	p	8	d	j	y	a	1
2	h	2	h	d	0	d	m	y	a	z	2
3	y	h	d	r	u	d	r	w	p	t	3
4	e	g	y	8	h	4	1	f	1	e	4
6	n	7	n	t	y	g	t	r	v	h	6
7	8	c	6	7	b	z	j	0	p	u	7
	A	B	C	D	E	F	G	H	J	K	



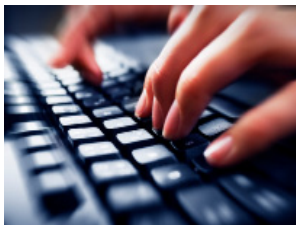
GridGo

est la version sans-tokens à la demande de GridID. Les grilles de sécurité sont affichées sur l'écran de l'utilisateur en temps réel à l'authentification.

Protégé par un PIN

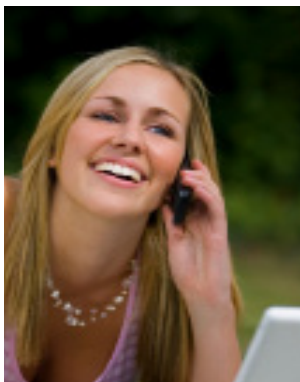
Les utilisateurs peuvent protéger leur grille de sécurité avec un code PIN ou un mot de passe. A chaque authentification, les utilisateurs génèrent un OTP en sélectionnant aléatoirement un point de départ sur la grille et en naviguant dedans en suivant un chemin secret qu'eux seuls connaissent. Cette technologie unique et brevetée protège les informations sur l'utilisateur même si la grille a été perdue ou volée.

TypeSense - VoiceSense - FaceSense



TypeSense est une solution d'authentification uniquement logicielle basée sur la reconnaissance de la frappe au clavier. Elle identifie de façon précise un utilisateur grâce à sa façon de saisir ses identifiants au clavier. TypeSense ne nécessite l'installation d'aucun matériel et fonctionne avec un clavier d'ordinateur standard. TypeSense est la seule authentification biométrique qui:

- peut être changée ou réinitialisée
- ne requiert aucun matériel spécial
- est complètement transparente
- peut être déployée rapidement

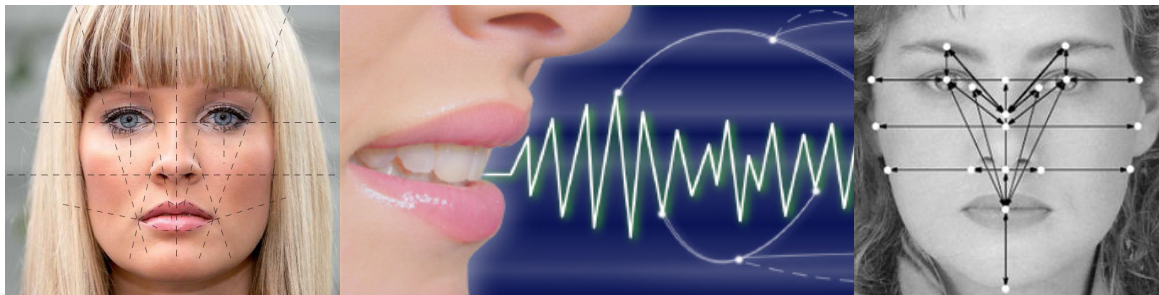


VoiceSense est un système biométrique vocal indépendant de la langue qui vérifie l'identité d'un utilisateur en temps réel grâce à la simple prononciation d'une phrase. VoiceSense est totalement indépendant de la langue ou de l'accent de l'utilisateur.

L'authentification par Voix est une technologie facile d'utilisation, non-intrusive et flexible. C'est une technologie très fiable et qui ne nécessite aucun équipement spécifique. L'omniprésence de micro sur les PC et les téléphones portables fait de l'authentification par la voix une méthode idéale d'authentification forte.

FaceSense est une technologie de pointe basée sur la reconnaissance faciale. C'est probablement la façon la plus naturelle de vérifier l'identité d'une personne. FaceSense ne requiert aucun matériel avancé car il est capable d'utiliser les appareils de capture d'image existants comme les Webcam ou les caméras intégrées aux téléphones portables.

MultiSense



MultiSense est une solution multi-biométrique qui combine et fusionne 3 technologies de biométrie différentes dans un seul système : reconnaissance faciale, vocale et de la frappe au clavier. L'utilisation du multi-biométrique permet de bénéficier de l'avantage de chaque technologie tout en dépassant les limitations de certaines d'entre elles. Cela ajoute ainsi précision et robustesse aux technologies de biométrie.

MultiSense est une solution d'authentification multi-facteurs facile d'utilisation. L'utilisateur peut par exemple regarder la caméra et prononcer une simple phrase.

- **Conviviale** : utilise un unique appareil comme une webcam afin de capturer plusieurs échantillon de traits biométriques comme l'image du visage et le son de la voix.
- **Résistant à l'usurpation** : demande à l'utilisateur de réciter une suite de mots aléatoire ce qui permet de s'assurer qu'un utilisateur "vivant" est présent.

DevicePass & FlashPass

Chaque ordinateur a ses propres caractéristiques. DevicePass crée une empreinte “digitale” pour l’ordinateur en utilisant les caractéristiques de celui-ci comme l’ID du disque dur, le numéro de série du CPU, l’adresse MAC réseau, etc. En combinant l’empreinte de l’ordinateur avec un utilisateur/mot de passe, il est possible de restreindre l’accès aux applications uniquement aux ordinateurs reconnus et aux utilisateurs authentifiés.

DevicePass fournit une solution sans token et transparente pour l’authentification forte des utilisateurs.



FlashPass transforme une clé USB standard en un token de sécurité en attachant l’identité de l’utilisateur à l’empreinte de la clé USB.

FlashPass ne requiert pas l’installation d’un logiciel spécifique sur les PCs. Les utilisateurs peuvent simplement insérer leur clé USB et être immédiatement authentifiés.

Authentification VPN/RADIUS

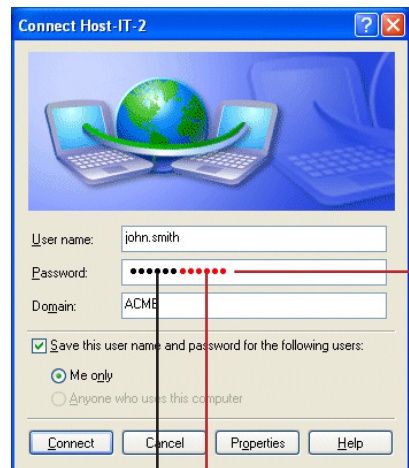
L'authentification des utilisateurs est le point faible des VPN. Les technologies VPN sont sécurisées mais uniquement au niveau de la transmission des données. Les VPN vérifient les utilisateurs avec un mot de passe statique, une approche qui offre une sécurité minimale car les mots de passe peuvent être facilement compromis. L'authentification forte des utilisateurs est la seule méthode efficace pour sécuriser les accès VPN nomades. L'authentification pour les VPN de Deepnet utilise les one-time passwords (OTP) générés par des tokens de sécurité comme SafeID ou MobileID pour offrir une sécurité optimale sans gêner l'utilisateur dans son activité. DualShield fournit un serveur RADIUS clé en main et conforme à la RFC 2865 qui supporte n'importe quel client ou application qui emploi le protocole RADIUS.

Intégration VPN transparente

L'authentification Deepnet pour VPN s'intègre avec n'importe quel pare-feu IPSEC ou SSLVPN comme :

- Cisco
- Nortel
- Checkpoint
- Juniper
- WatchGuard
- Cyberoam
- SonicWave
- AEP
- Aventail
- F5

En utilisant les OTP, les utilisateurs n'ont rien à installer. Ils continuent à utiliser le client VPN dont ils ont l'habitude et vont simplement saisir un OTP ou la combinaison OTP + mot de passe statique dans les champs de saisie du mot de passe.



One Time Password
Mot de passe statique

Authentification Windows/Linux

L'authentification Deepnet pour Windows est conçue pour aider les entreprises à s'assurer que les ressources réseaux ne sont accessibles qu'aux utilisateurs autorisés, que ce soit en travaillant localement derrière le pare-feu ou en travaillant à distance grâce au bureau à distance. C'est une solution complète qui renforce l'authentification aux domaines Windows ainsi qu'aux postes de travail grâce à l'authentification à deux facteurs.



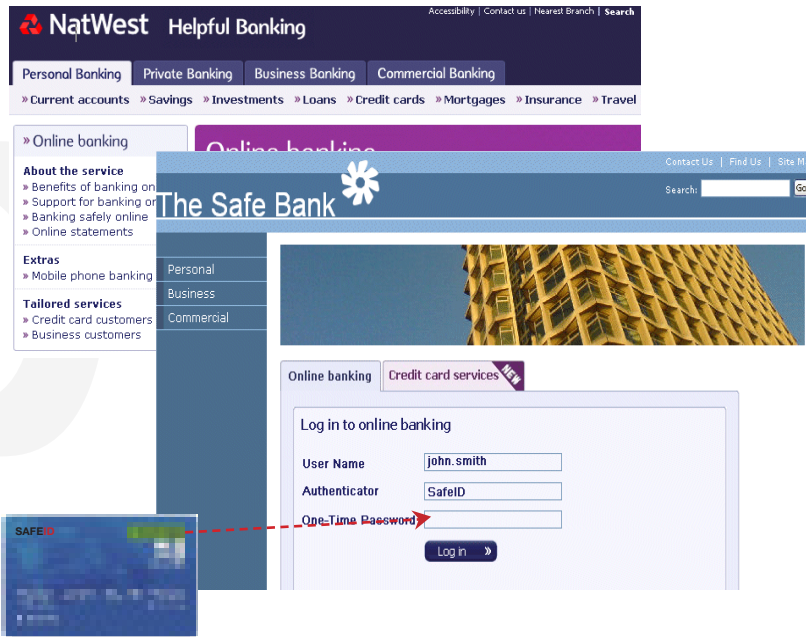
Support:

- Accès local
- Bureau à distance
- Terminal Server
- Active Directory
- Windows 2000, XP, Vista, Windows 7
- Windows 32-bit and 64-bit
- Authentification en ligne et hors ligne

Les systèmes Linux et les applications qui supportent PAM peuvent également s'authentifier auprès de DualShield

Authentification Web

L'authentification Deepnet pour le Web est conçue pour aider le e-commerce et les entreprises à contrôler l'accès à des zones restreintes de leurs sites Internet. Seuls sont autorisés les utilisateurs qui fournissent une authentification à deux facteurs, grâce à l'utilisation d'une des nombreuses solutions de tokens de Deepnet.

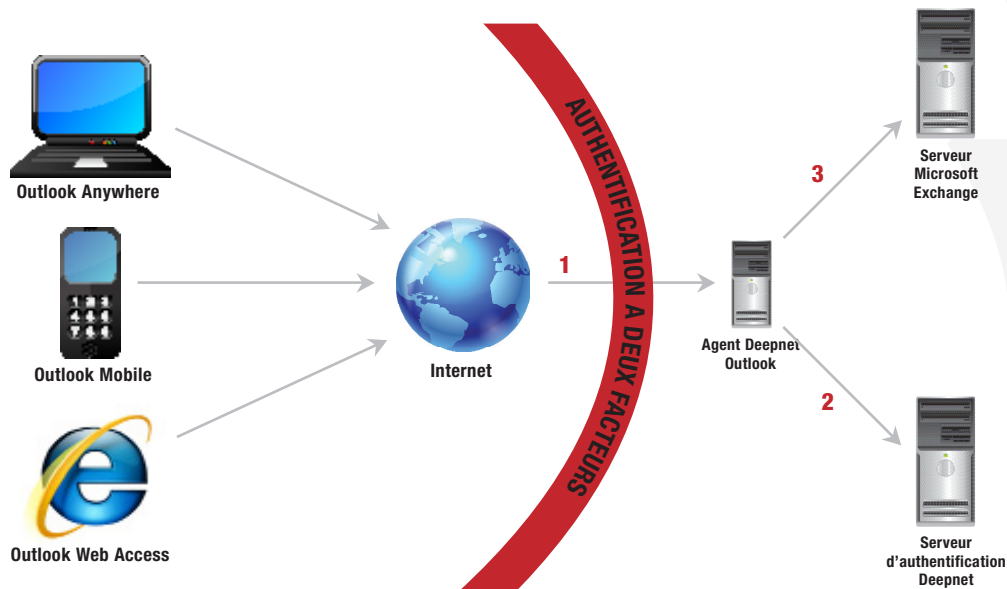


DualShield fournit une SDK/API afin de permettre aux développeurs d'intégrer l'authentification forte à leurs applications Web.

Authentification Outlook

L'authentification Deepnet pour Outlook permet de sécuriser l'accès aux solutions Outlook suivantes:

- Interface Web Outlook
- Outlook Anywhere
- Outlook Mobile pour Exchange ActiveSync

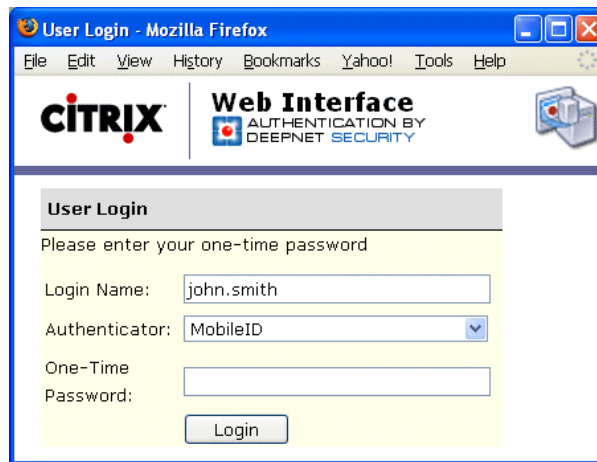
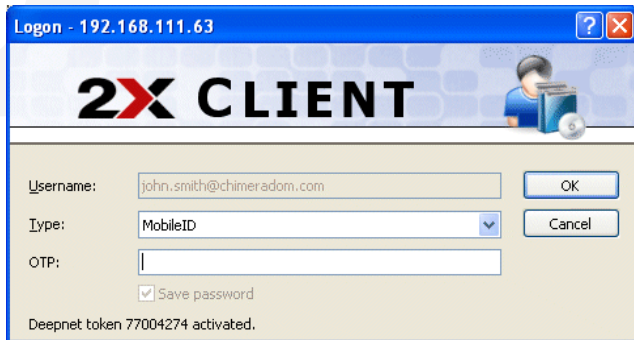


Citrix & 2X

Alors que Citrix a rendu plus simple l'accès aux informations critiques, utiliser une authentification par simple mot de passe peut être risqué pour l'entreprise. Deepnet DualShield améliore la sécurité des solutions Citrix en authentifiant les utilisateurs grâce à un système d'authentification forte.

Deepnet DualShield permet d'apporter un accès sécurisé aux solutions Citrix suivantes :

- Interface Web Citrix pour XenApp
- Citrix Access Gateway avec Advanced Access Control
- NetScaler SSL VPN



2X fournit une famille de logiciel pour serveurs d'entreprise qui permet la virtualisation des postes de travail et le streaming des applications sur des PCs standard ou des clients légers. Intégrée nativement dans le coeur du système 2X, l'authentification Deepnet améliore la sécurité pour toutes les solutions 2X en authentifiant l'utilisateur sur une plateforme d'authentification forte.

"La solution est facile à installer et à administrer, elle est facile d'utilisation et fournit un large support de tokens et d'options d'authentification. Le prix est très attractif pour les petites et les grandes entreprises" – SC Magazine

"De toutes les méthodes d'authentification que nous avons testées, c'est de loin la meilleure..." – CoinCo Inc

"Nous avons débuté un processus de test de différentes solutions; cela incluait Deepnet, RSA et d'autres solutions importantes. Durant ces tests nous avons trouvé que la flexibilité et la facilité d'utilisation de la plateforme d'authentification unifiée Deepnet satisfaisait nos besoins bien mieux que les compétiteurs..." – Teign Housing

"Nous avons regardé un certains nombre de solutions comme Secure Computing, RSA et Swivel. Deepnet fournit la plus grande flexibilité grâce au nombre d'applications qui peuvent être sécurisées et le nombre de méthodes d'authentification possibles..." – NHS



Partenaires



Clients



et des centaines d'autres...

Deepnet Security

www.deepnetsecurity.com

info@deepnetsecurity.com

US: +1 714 937 2051

UK: +44 208 343 9663