PRÉSENTATION DE LA GAMME

Authentification

Les entreprises sont confrontées à de nouveaux défis en matière de contrôle des accès. En effet, les appareils mobiles s'imposent de plus en plus comme l'outil informatique de prédilection à l'heure où la majorité des entreprises optent pour l'utilisation d'applications SaaS et Cloud et où les menaces prolifèrent.

- **Adoption rapide d'applications SaaS et Cloud :** L'utilisation d'applications Cloud permet à tous les utilisateurs de travailler à distance. Même si les entreprises adoptent de plus en plus les applications SaaS, elles n'abandonnent pas pour autant leurs systèmes locaux traditionnels. Il est donc essentiel d'étendre les identités de l'entreprise au Cloud.
- **Mobilité et grande variété de terminaux :** En raison de l'augmentation en flèche du nombre de terminaux se connectant aux systèmes d'entreprise, il est de plus en plus compliqué pour les entreprises de mettre en place des méthodes uniformes de contrôle d'accès et d'authentification de ces terminaux.
- **Vecteurs de menaces :** Les cybercriminels ciblent les institutions financières mais aussi les sociétés dont la propriété intellectuelle est de très grande valeur, les organisations gouvernementales et les entreprises possédant des informations personnelles sensibles.

Face à ces enjeux, la mise en place d'une authentification forte unifiée, gérée de manière centralisée et facile à délivrer, ainsi qu'une connexion fédérée est vitale à la sécurité des systèmes de l'entreprise.

Avantages

Entièrement automatisée

- Réduit de manière drastique le coût d'approvisionnement, d'administration et de gestion des utilisateurs et des tokens.

Large choix de tokens

- Solutions matérielles, logicielles, SMS, OOB (hors bande) et sans token permettant de répondre à une multitude de scénarios d'utilisation et de niveaux de risques.

Nombreux scénarios d'utilisation

- Sécurise tout l'écosystème de l'entreprise (local, SaaS, VPN, environnements virtuels et Cloud privés).

Réduction du CTP

- Réduit considérablement le coût total de possession par rapport aux environnements d'authentification forte traditionnels.

Nouvelle génération de solutions d'authentification de Gemalto

Fortes de plus de 17 ans d'expérience sur le marché de l'authentification, les solutions d'authentification SafeNet de Gemalto sont plébiscitées par des milliers d'entreprises à travers le monde.

Gemalto aide les entreprises à adapter leurs activités et leur sécurité pour répondre aux défis du Cloud, de la mobilité et de la prolifération des menaces en leur fournissant des

solutions d'authentification d'une grande souplesse et simplicité d'utilisation. Gemalto simplifie la mise en place et la gestion de l'authentification grâce à des processus automatisés qui réduisent de manière drastique la durée et le coût de l'approvisionnement, l'administration et la gestion des utilisateurs par rapport aux modèles d'authentification traditionnels.

Nous offrons un large éventail de méthodes et de formats d'authentification accompagnés de fonctions de connexion fédérée et de modèles de tarifs souples. Nous sommes en mesure de répondre aux différents scénarios d'utilisation et niveaux de fiabilité de nos clients et aux nombreux vecteurs de menace grâce à des politiques unifiées et gérées de manière centralisée. Un seul serveur backend d'authentification installé dans le Cloud ou localement est requis pour traiter toutes ces opérations.

Plates-formes d'authentification Gemalto

Gemalto SafeNet Authentication Service

Gemalto SafeNet Authentication Service offre une authentification sous forme de service hautement sécurisée et entièrement automatisée ainsi qu'une connexion fédérée avec des options de tokens flexibles adaptées aux besoins uniques de votre société pour une réduction significative du coût total de possession.

L'authentification forte est facilitée par la souplesse et l'évolutivité des flux de travail automatisés et par la prise en charge de tokens de fournisseurs tiers et de larges interfaces de programmation (API). En outre, les capacités de gestion et les processus sont entièrement automatisés et personnalisables — pour une expérience utilisateur riche et transparente.

Aucune infrastructure n'est nécessaire. SafeNet Authentication Service permet une migration rapide vers un environnement Cloud multi-niveaux et collectif. Il assure la protection des applications Cloud et locales, des réseaux, des utilisateurs et des appareils.

Gemalto SafeNet Authentication Manager

Gemalto SafeNet Authentication Manager est un serveur d'authentification polyvalent qui permet aux entreprises de mettre en place une stratégie d'authentification forte et évolutive pour sécuriser l'accès local et distant à de nombreuses ressources professionnelles à l'aide d'un seul serveur backend d'authentification.

SafeNet Authentication Manager prend en charge le plus large éventail de méthodes et de formats d'authentification, notamment l'authentification contextuelle, avec des fonctionnalités à plusieurs niveaux dont le mot de passe à usage unique OTP, les tokens à certificats X.509 et les tokens logiciels, afin de permettre aux organisations de bénéficier de différents niveaux de fiabilité et de traiter de nombreux scénarios d'utilisation.

Grâce à la gestion unifiée des politiques de sécurité pour les applications SaaS, les ressources réseau et les appareils mobiles et à la prise en charge d'applications de sécurité de pointe, SafeNet Authentication Manager permet aux entreprises d'adapter leurs besoins actuels et futurs en matière d'accès sécurisé.

Authentificateurs SafeNet de Gemalto

Le plus large éventail de méthodes et de formats d'authentification du marché. Nous sommes en mesure de répondre aux différents scénarios d'utilisation et niveaux de fiabilité de nos clients et aux nombreux vecteurs de menace grâce à des politiques unifiées et gérées de manière centralisée.

Authentificateurs OTP

> Une large gamme de tokens matériels et logiciels basés sur le temps/ les événements et prenant en charge le challenge/response sont disponibles pour l'accès à distance et réseau.

Authentificateurs à base de certificats

> Les formats USB et smartcard prennent en charge l'authentification haute fiabilité et les applications de sécurité de pointe.

Téléphone en tant que token

> Solutions logicielles pour toutes les plus grandes plates-formes mobiles et pour les postes de travail Windows et Mac.

Hors bande (OOB)

> La méthode d'authentification OOB par SMS et email facilite l'envoi du mot de passe.

Authentification contextuelle

> Accès à distance pratique, rentable et sécurisé grâce à l'authentification forte sans token.

Grid Tokens

> GrIDsure génère un mot de passe à usage unique sans utiliser de tokens matériels ou logiciels.

Nous contacter : retrouvez toutes les coordonnées de nos filiales sur www.safenet-inc.fr
Nous suivre : data-protection.safenet-inc.com

GEMALTO.COM

gemalto
security to be free