i-Trust

Contrôle d'accès de vos applications Web

Sécurisé, Simple et Unique

Bénéfices

- **Sécurité**
  Contrôle d'accès unifié et renforcé
- **Transparence**
  S'adapte à l'existant technique et organisationnel
- **Facilité d'utilisation**
  Point d'accès et Authentification uniques pour les utilisateurs (Web Single Sign On)
- **Approche structurante**
  Homogénéité et contrôle global des accès applicatifs

L'authentification : composante critique des applications

Du point de vue de l'utilisateur la performance d'une application est une affaire de rapidité, de simplicité d'emploi et de facilité d'accès. Ce dernier critère revêt une importance grandissante quand le nombre d'applications augmente : multiplication des points d'accès, des méthodes, des comptes et mots de passe…

Du point de vue de l'exploitant, ce constat prend encore plus de force. La gestion de contrôles d'accès multiples, réalisés selon des schémas d'authentification différents, est d'une part un casse-tête administratif et d'autre part représente un risque potentiel fort parce que difficilement contrôlable.

Simplicité et cohérence pour gagner en efficacité et en sécurité

L'idée innovante apportée par Bee Ware est à la fois de déporter et de centraliser l'authentification au périmètre du réseau sur une passerelle de sécurité applicative.

Ce modèle d'architecture s'affranchit de la diversité et de l'éventuelle fragilité des authentifications réalisées nativement par les applications.

Et c'est toute l'Entreprise qui y gagne :

- Les responsables de l'entreprise, qui décident eux-mêmes le niveau d'authentification souhaité et ne subissent plus celui imposé par les applications
- Les exploitants, qui peuvent concentrer leur attention sur la supervision d'un point d'accès unique et homogène
- Les utilisateurs, qui bénéficient du confort d'utilisation d'une solution de Single Sign On.

contact@bee-ware.net • www.bee-ware.net
FRANCE : **+33 (0)1 41 03 14 83**

À propos de Bee Ware :

Bee Ware est un éditeur spécialisé dans la sécurisation et l'optimisation des applications Web. Disponibles sous forme d'Appliance, les solutions Bee Ware garantissent à la fois les performances et la confiance permettant de bénéficier des technologies Web en toute sérénité.

BeeWare
Delivering Confidence in Web Applications

i-Trust

Simplicité et transparence

En se focalisant sur les applications Web et en apportant un niveau d'automatisation inégalé grâce à sa technologie "d'Auto-Apprentissage", Bee Ware a conçu une solution "facile", c'est-à-dire qui ne soit pas un casse-tête pour les utilisateurs, ni une nouvelle charge de travail pour les exploitants.

FACILE À INSTALLER

i-Trust s'installe de façon simple et rapide. La solution peut soit utiliser un annuaire de compte existant (LDAP, Radius…) soit constituer son propre annuaire interne par importation de données. La synchronisation avec les comptes utilisateurs préalablement gérés par les applications elles-mêmes s'effectue de façon transparente grâce à la fonction d'auto-apprentissage incluse avec i-Trust.

FACILE À EXPLOITER

Les opérations de maintenance et de suivi sont tout aussi simples avec i-Trust. En effet, la fonction d'auto-apprentissage permet la synchronisation automatique des mots de passe entre les applications et la base centralisée, évitant ainsi les fastidieuses interventions des exploitants.

i-Trust + i-Sentry

La solution i-Trust fonctionne soit de façon autonome, soit installée en tant que module complémentaire de i-Sentry. L'offre complète représente une solution de sécurité Web globale avec notamment : Protection contre les attaques, Détection des vulnérabilités applicatives, Politique granulaire d'accès basée objet, Optimisation des performances et Authentification renforcée et unifiée.

Caractéristiques

Gamme de 6 modèles selon performance
Appliance Sécurisé format 1U ou 2U
Accélération SSL Hardware
Management Web (SSL)
Supervision SNMP et Syslog
Haute Disponibilité (option)

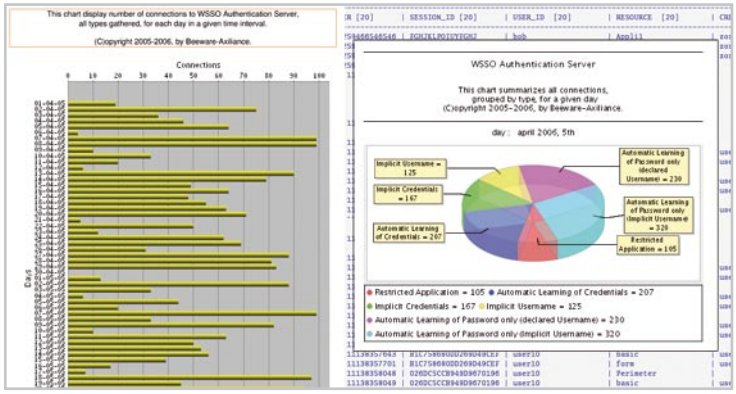
Fonctionnalités

• Authentifications Périmètriques

- Formulaire Login / Password
  Base de comptes interne à i-Trust
- Authentification LDAP
  Accès annuaire LDAP externe
- Authentification RADIUS
  Accès base de comptes Radius externe
- Authentification X.509 Client
  Accès à une PKI ou variante interne LDAP ou Radius
- Authentification via offre tierce partie
  RSA SecurID – Elcard…
- Authentification GIP CPS
  Carte des Professionnels de la Santé

• Authentifications Applicatives

- HTTP Basic, DIGEST, NTLM
- Formulaire HTML
- Headers Paramétrables



Mode opératoire

1 La demande de connexion de l'utilisateur est interceptée par l'agent i-Trust situé sur la passerelle applicative : Tant qu'il n'est pas authentifié l'utilisateur ne peut ni accéder ni même voir les serveurs applicatifs.

2 Le serveur d'authentification i-Trust obtient les crédentiels de l'utilisateur (base de comptes interne ou externe) et réalise le contrôle d'accès périmètrique en appliquant le modèle d'authentification choisi par l'entreprise et non pas ceux fournis par les applications.

3 Sur la base des credentiels obtenus, le serveur i-Trust "joue" de façon transparente une ou plusieurs authentifications applicatives, respectant ainsi l'organisation existante des applications.

Après une authentification unique et sécurisée, réalisée au périmètre du réseau par la passerelle applicative, l'utilisateur a maintenant accès à l'ensemble de ses applications.