IIGF18 - Automatisation et Sécurisation de l'accès à l'information

Frédéric MICHEL

IBM Tivoli Security

Smarter Planet

Agenda

- La vision d'IBM de la sécurité informatique
- Le Cadre de Référence Sécurité
- Les offres Sécurité d'IBM
  - Gestion des Identités et des Accès
  - Protection des applications et des données
  - Protection des postes
  - Protection des infrastructures techniques
  - Supervision de l'activité de sécurité

Bienvenue dans **une planète plus intelligente** …

Globalisation et virtualisation des ressources

Milliards d'équipements et d'individus accèdent au web

Accès à l'information En temps réel

Nouvelles formes d'échange et de collaboration

+ de possibilités
+ de complexité
Nouveaux risques

Les menaces augmentent.. Impactant les niveaux de services, les coûts et l'activité. Il existe une multitude de scénarios de menaces …

Menaces Externes

▪ Pannes d'électricité ▪ Désastres naturels ▪ Bouleversements économiques	▪ Malware ▪ Déni de service ▪ Attaques sophistiquées et organisées
▪ Systèmes non patchés ▪ Vulnérabilité du code ▪ Pas contrôle des changements ▪ Erreur humaine	▪ "Back doors" créées par des développeurs ▪ Vol de données ▪ Fraudeurs internes

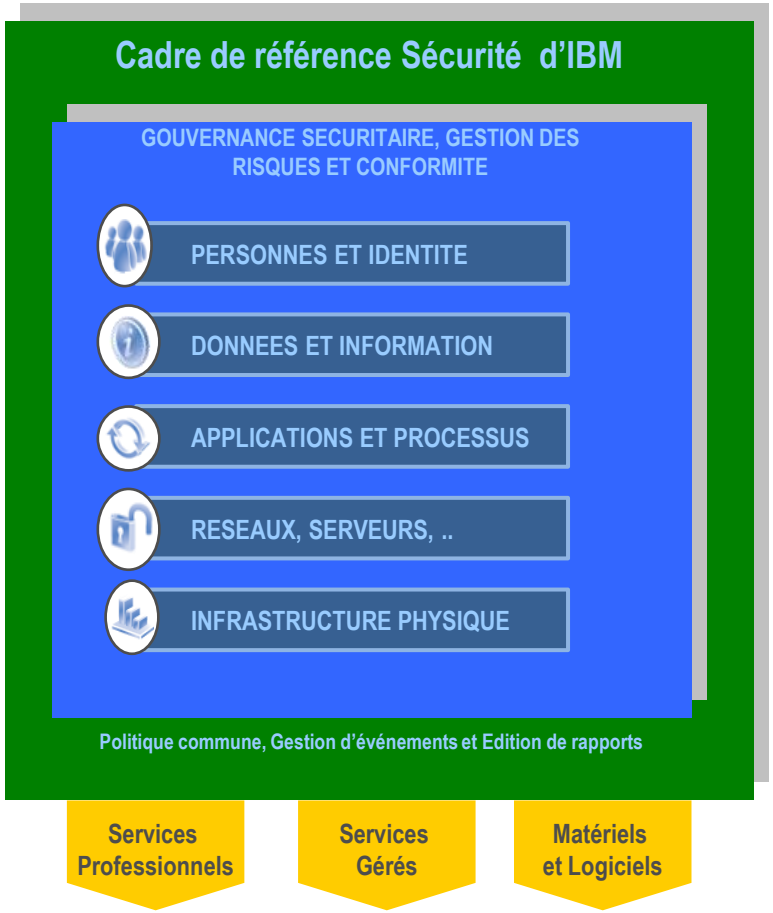
Par inadvertance ***Intentionnelles***

Menaces internes

IBM se donne les moyens pour proposer des solutions de sécurité globale, permettant à nos clients d'assurer la gouvernance de leur sécurité, de gérer les risques et la conformité.

IBM Research reconnu comme "**Top Privacy Inventeurs**" en 2009

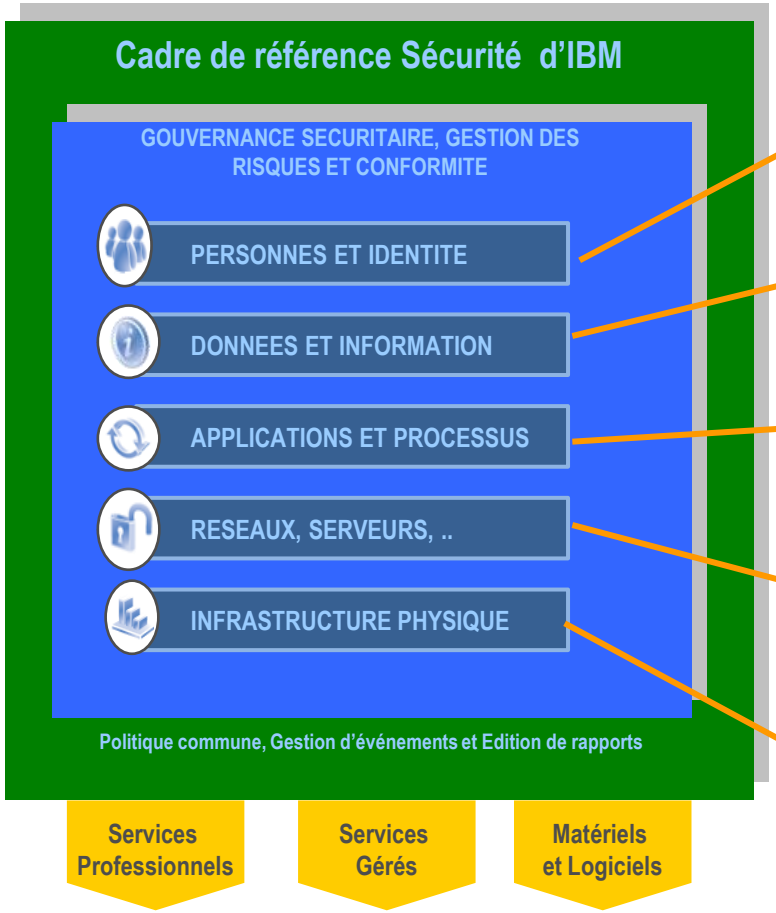
- Le seul spécialiste de sécurité qui s'est doté d'un cadre de référence permettant à ses clients de gérer les risques **de bout en bout** sur les 5 domaines de la sécurité des SI
- **15,000** chercheurs, développeurs et spécialistes au niveau de la sécurité des systèmes d'information
- **3,000+** brevets en sécurité et gestion des risques
- **2000+** références sécurité et **50+** études de cas publiées
- Nombreuses acquisitions
- Nous gérons 13 **Milliards** d'événements de sécurité par jour chez plus de 3 700 clients
- **40+** années de succès démontré dans le domaine des environnement zSeries



Agenda

- La vision d'IBM de la sécurité informatique
- Le Cadre de Référence Sécurité
- Les offres Sécurité d'IBM
  - Gestion des Identités et des Accès
  - Protection des applications et des données
  - Protection des postes
  - Protection des infrastructures techniques
  - Supervision de l'activité de sécurité

L'objectif principal d'IBM est de protéger intégralement ses clients des multiples menaces liées à la dématérialisation et au cloud, pour leur permettre d'escompter les bénéfices qualitatifs et tangibles.



Fournir aux utilisateurs les ressources informatiques dont ils ont droit pour exercer à l'instant T.
Prouver la conformité par rapport à la politique de sécurité

Comprendre, déployer et tester de manière appropriée les contrôles d'accès et d'usage de données sensibles

Protéger les applications contre les failles de sécurité sur la durée, sécuriser les webservices

Protéger le réseau des entreprises, les serveurs, les environnements virtualisés et les postes de travail

Protéger les accès physiques par les systèmes de contrôles d'accès, la vidéosurveillance Intelligente et les postes de commandement

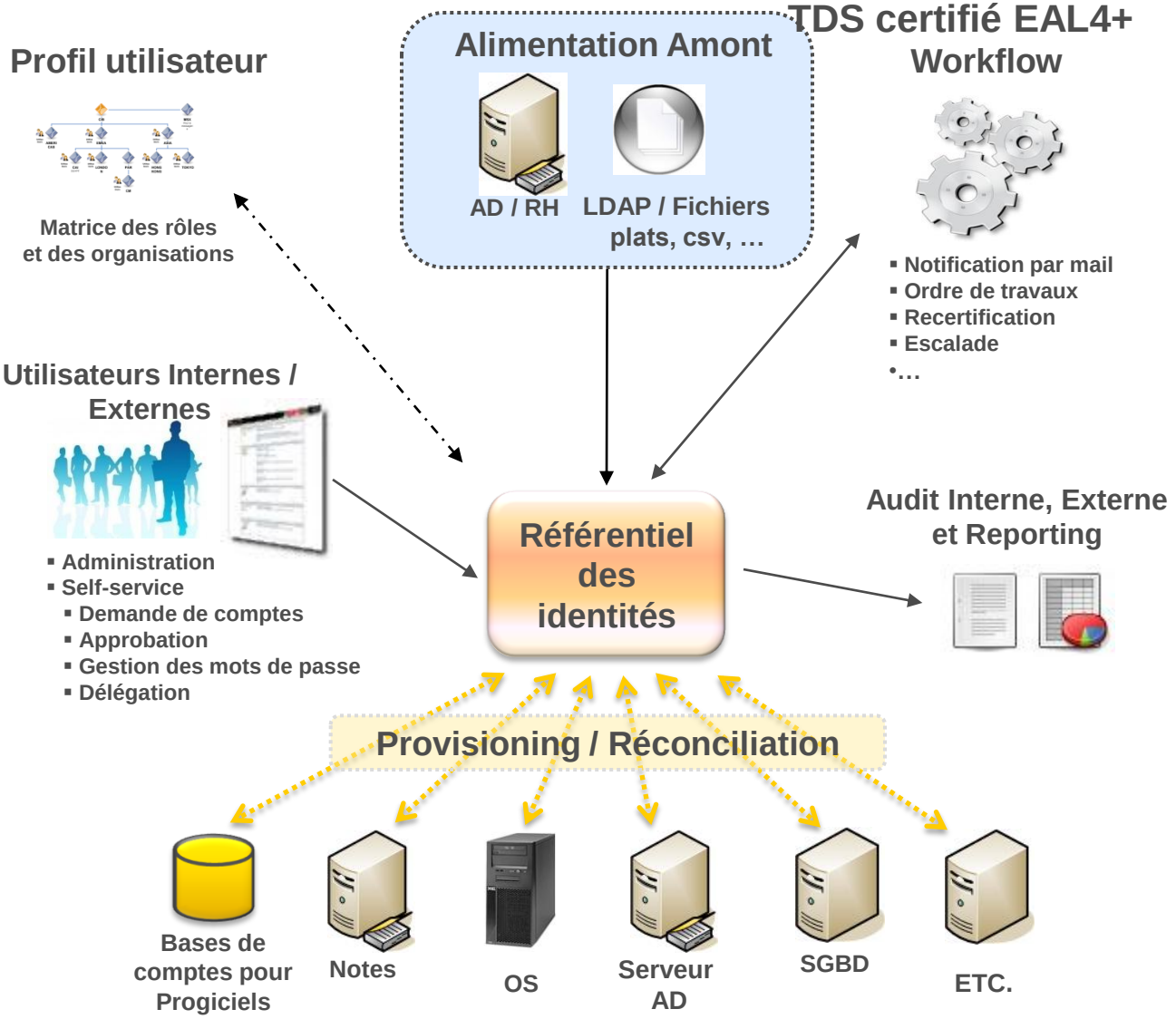
Agenda

- La vision d'IBM de la sécurité informatique
- Le Cadre de Référence Sécurité
- Les offres Sécurité d'IBM
  - Gestion des Identités et des Accès
  - Protection des applications et des données
  - Protection des postes
  - Protection des infrastructures techniques
  - Supervision de l'activité de sécurité

Tivoli Identity Manager (TIM)

Gestion des identités

- Gestion centralisée et automatisée des différentes ressources
- Modèle de rôle et d'habilitation normalisé au standard RBAC
- Automatisation des tâches d'administration
- Réduction des délais de provisioning
- Self service : Réduction du coût pour le Help Desk
- Audit et reporting des habilitations
- Gestion de la conformité
- Moteur de workflow adaptable aux processus

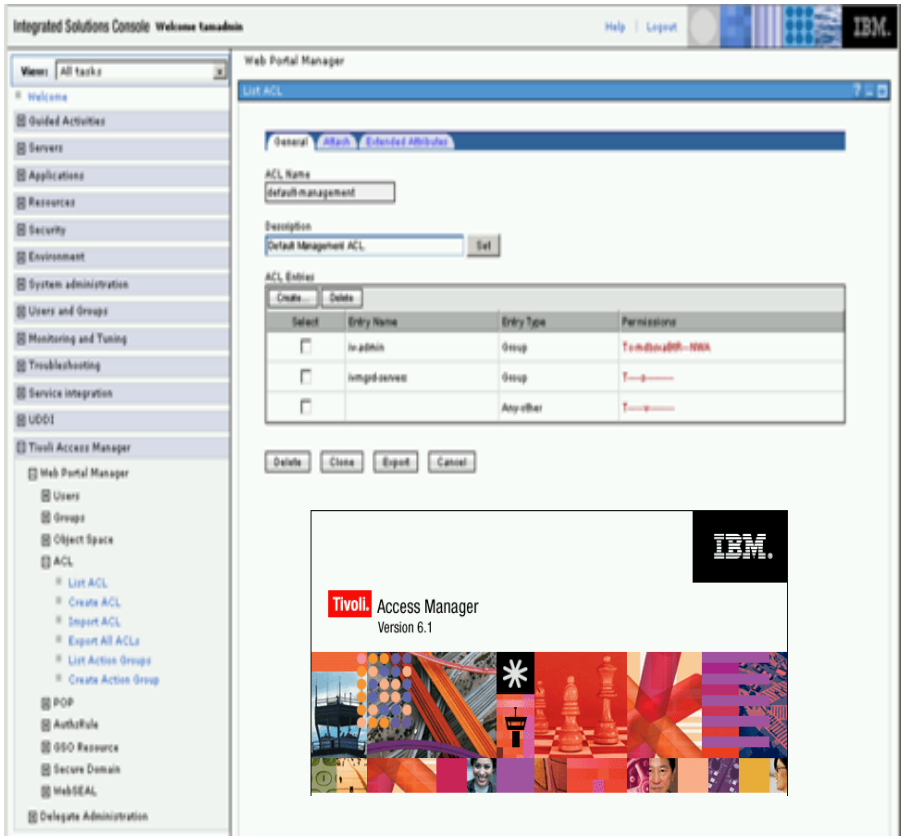


TAM eb

Gestion des accès aux applications Web Intranet et Extranet

Certifié EAL3+
Intégré avec SafeSign

- Solution de SSO d'applications Web et portail
- Facilité d'intégration au SI, au système de gestion des identités
- Supporte des dizaines de millions d'utilisateurs
- Accepte un grand nombre de solutions d'authentification forte
- Offre une solution centrale d'autorisation et d'audit pour les déploiements en entreprise
- Minimise les risques de XSS et XSRF
- Visibilité : propose une vue unique des utilisateurs d'un grand nombre d'applications: de la messagerie à l'ERP
- Contrôle :authentification flexible et SSO entre plusieurs communautés d'utilisateurs
- Automatisation : facile à déployer sur un grand nombre d'applications et à gérer



TAM ESSO v8

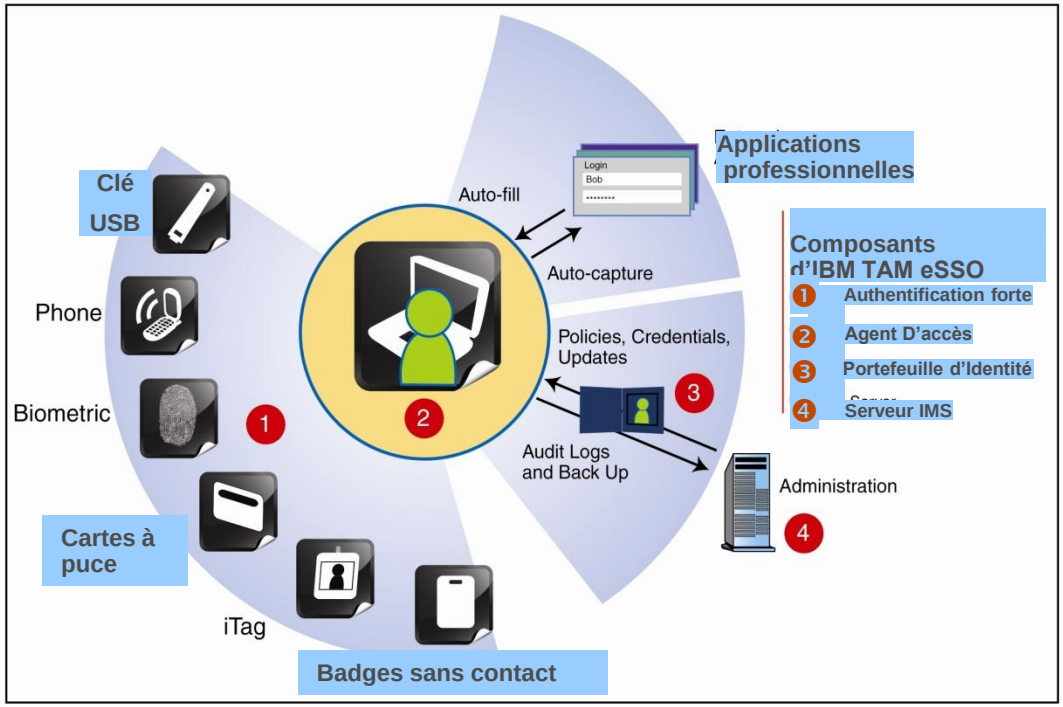
Gestion des accès aux applications d'entreprise

TAM ESSO offre :

- **SSO aux applications professionnelles (progiciels métiers, logiciels, développements spécifiques, windows, citrix..)**
- **Authentification forte**
- **Automatisation des worlfows de sécurité et des accès**
- **Changement d'utilisateurs rapides**
- **Traçabilité et auditabilité des accès**
- **Gestion centralisée des identités et de politiques de sécurité**

Sans changement de l'infrastructure.

En cours de certification EAL4+



Agenda

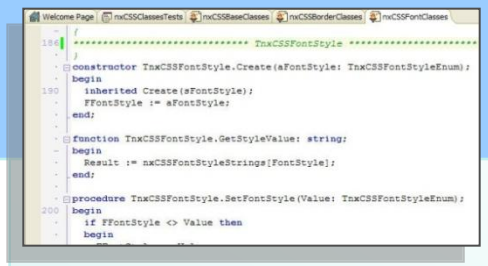
- La vision d'IBM de la sécurité informatique
- Le Cadre de Référence Sécurité
- Les offres Sécurité d'IBM
  - Gestion des Identités et des Accès
  - Protection des applications et des données
  - Protection des postes
  - Protection des infrastructures techniques
  - Supervision de l'activité de sécurité

Technologies de test de la Sécurité applicative ...

Deux approches combinées pour une plus grande précision

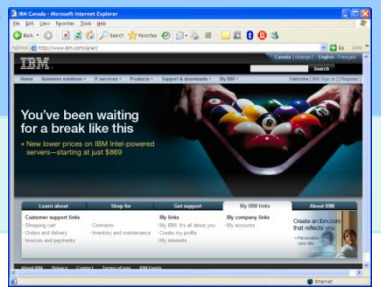
Analyse Statique (White Box)

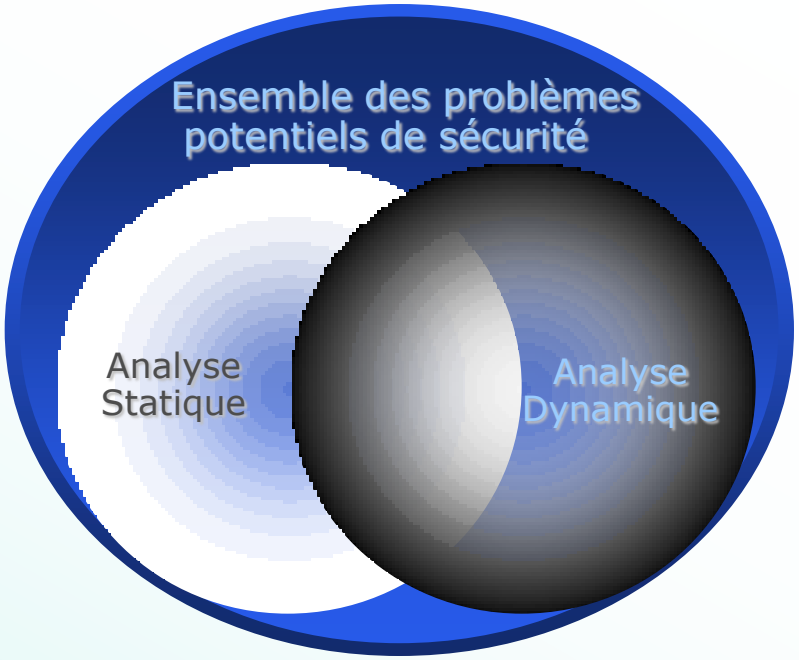
- Parcours du code source pour identifier les failles de sécurité
- Automatisation de l'audit de code



Analyse Dynamique (Black Box)

- Réalise une analyse axée sur la sécurité d'une application compilée et déployée
- Automatisation des attaques de hackers





AppScan

XML Security Gateway XS40

Protection des Webservices et des echanges de données

Certifié EAL4

- Centralise la sécurité XML et l'application des politiques de sécurité
- Appliance de sécurité durcie pour des déploiements DMZ
- Interfaces de configuration simplifiées pour minimiser le besoin de compétences SOA
- Interopérabilité facilitant l'intégration des webservices avec d'autres acteurs de la santé, des partenaires, de fournisseurs
- Authentification et autorisation fine contre les moteurs des tiers

Sécurise les applications de nouvelle génération avec un firewall XML and SOAP firewall qui filtre le trafic à très grande vitesse.

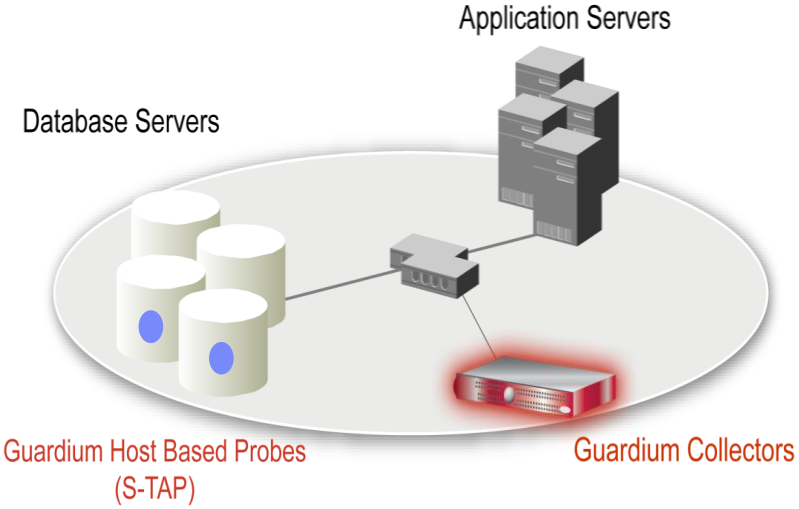
Valide les schémas et messages XML, protège contre les attaques XML, temporise les débordements, ou les vulnérabilités de documents XML erronés.

Fournit une sécurité au niveau des champs XML grâce au chiffrement, déchiffrement, à la signature et vérification d'un message entier ou d'un champ du message.

Supporte une variété de mécanismes de contrôles d'accès et peut contrôler l'accès en rejetant tous les messages non signés, et en vérifiant ou injectant des assertions SAML.

- **Garantir la confidentialité et l'intégrité des données**
  - Appliquer les contrôles d'accès et de de changements sur les systèmes critiques
  - Au travers de toutes les applications et les base de données
    - Oracle, SQL Server, IBM DB2 & Informix, Sybase, MySQL, Teradata
    - SAP, Oracle Financials, PeopleSoft, Siebel, Business Objects, …

- **Accroitre l'efficacité opérationnelle**
  - Automatiser, simplifier et centraliser les contrôles internes
  - Au travers des environnements hétérogènes & répartis
  - Identifier et remédier rapidement les problèmes de performance & les erreurs application
  - Plateforme évolutive pour faire face aux centres de données les + exigeants
- **Pas de dégradation de l'infrastructure ou des process business**
  - Architecture non intrusive et sans impact sur la production
  - Pas de changements nécessaires sur les applications et les bases de donnees

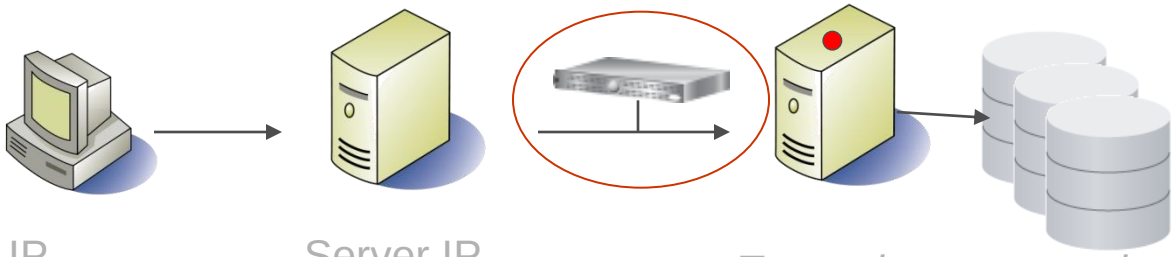


ORACLE
IBM DB2
SQL Server
TERADATA
SYBASE
MySQL
Informix

Guardium
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Audits Précis et fins

Avec Guardium, tout le traffic SQL est analysé et filtré en temps-réel et dans le contexte afin de fournir les informations spécifiques requises par les auditeurs. Bien + d'informations et de granularité que dans des logs.



Client IP
OS user ID
Client host name
Domain login
Client OS
MAC
TTL
Origin
Failed logins

Server IP
Server port
Server name
Session
SQL patterns
Network protocol
Server OS
Timestamp
App user ID
Access programs

Toutes les commandes SQL
Fields
Objects
Verbs
DDL
DML
DCL
DB user ID
DB version
DB type
DB protocol
Ports
SQL errors
SELECTs
Bind values

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Agenda

- La vision d'IBM de la sécurité informatique
- Le Cadre de Référence Sécurité
- Les offres Sécurité d'IBM
  - Gestion des Identités et des Accès
  - Protection des applications et des données
  - Protection des postes
  - Protection des infrastructures techniques
  - Supervision de l'activité de sécurité

Endpoint management: Les trois Cs

Patch is #2 client concern according to Gartner report. (2009)

Complexité

- Gérer la complexité, Simplifier et Automatiser
  - Coordination entre les processus métier de votre organisation
  - Endpoints, réseaux, applications et OS hétérogènes

Compliance

- Assurer la Conformité, Réduire les risques
  - Vulnérabilités de sécurité
  - Inventaire imprécis
  - Conformité des réglementations de l'industrie et audit (COBIT, SOX, HIPAA, et plus)

Coût

- Reduire le TCO & les Coûts Opérationnels
  - Supprimer les interventions manuelles
  - Supprimer les diverses configurations non nécessaires
  - Améliorer l'éfficacité

Simplifier les Operations et la Securité sur les Endpoints

Tivoli Endpoint Manager permet aux clients de consolider les opérations IT et la sécurité à partir d'une vue unique, dans un modèle de prestation et d'offres logiciels.

- **Aide à fournir …**
  - Visiblité totale
  - Contôle qualité
  - Vitesse de remédiation
  - Haute évolution
  - Framework polyvalent
  - "Rapid time to value"
  - Réduction des coûts

- **Grâce à l'union de….**
  - la gestion des configurations et des vulnérabilités
  - la sécurité
  - la gestion cycles de vie des systèmes,
  - la protection du endpoint
  - la gestion d'alimentation

- **Résultant en ….**
  - Economies immédiates
  - Simplifier les opérations
  - Réduire les risques

BigFix Large Enterprise Customers *Sample*	Devices
Fiberlink	800,000
US Department of Veterans Affairs	470,000
Intel Corporation	350,000
Los Angeles Unified School District	276,000
Kaiser Permanente	241,900
Wal-Mart Stores	200,000
Verizon Communications Inc.	186,000
Sinopec	181,200
Merrill Lynch / Bank of America	140,000
Miami-Dade Unified School District	121,000
Deutsche Bank AG	110,000
China Ministry of Rails	103,000
Morgan Stanley and Co Incorporated	100,000
US Federal Bureau of Investigation	100,000

Les éléments de la plateforme Tivoli Endpoint Manager

Agent intelligent unique

- Auto-évaluation en continu
- Politiques appliquées en continu
- Impact minimal sur le système (<2% cpu)

Console et serveur unique

- Sécurité forte, haute disponiblité
- Consolider les analyses, les données et les rapports
- Gestion >250k endpoints

Language de politiques puissants (Fixlets)

- Milliers de politiques “Out of the Box”
- Best practices pour la sécurité et l’opérationnelle
- Création simple de politiques personnalisées
- Extensible/ appliqué à travers toutes les platefomes

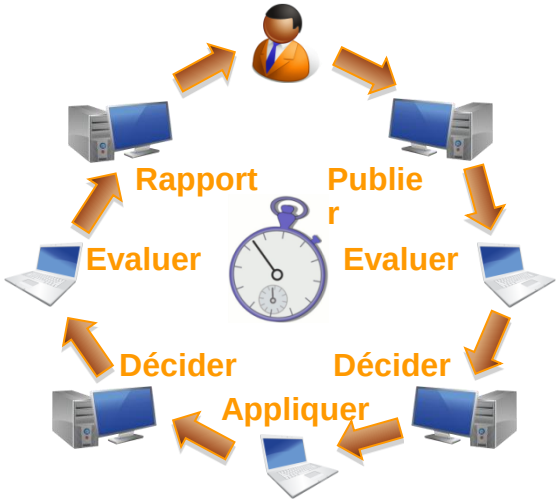
Une machine gérée par TEM peut devenir un relais en quelques minutes

Infrastructure virtuelle

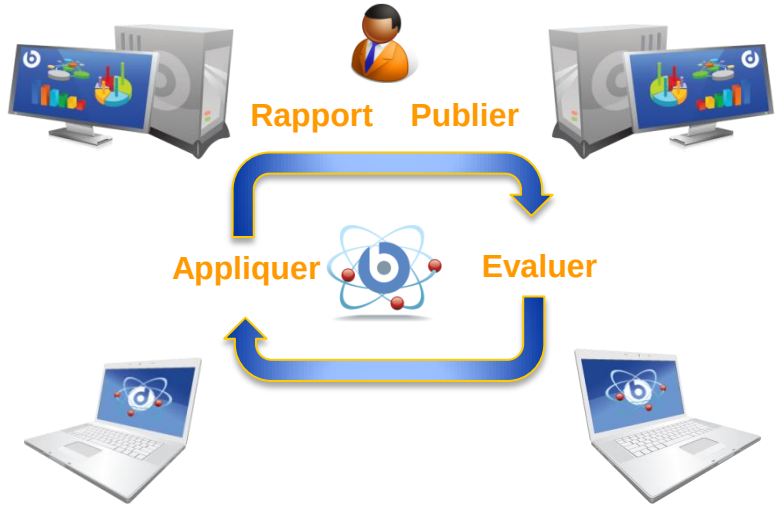
- Désigner n’importe quel agent TEM comme relais ou point d’analyse
- Construit en redondance
- Tirer parti des systèmes existants / infrastructure partagée

Closed Loop Speed is Our Advantage

Solutions traditionnelles



TEM



Challenge	Outil clients / serveurs traditionnelles	Plateforme TEM
Compléter la boucle d'application des politiques	Tout est controllé par le serveur, ce qui est lent.	Distribué l'information avec un agent intelligent et universel
Augmenter la rapidité et la précision de vos connaissances	Cela peut prendre des jours pour terminer avec précision la boucle d'execution	L'application de politiques est accomplie et prouvée en quelques minutes au lieu de jours
L'evolutivité ne peut être atteint sans gros investissements d'infrastructure	Les Administrateurs doivent encore gérer les outils au lieu d'être productif	La distribution et l'évolution des moyens de traitement sont illimités
Ajuster les politiques systèmes en fonction de l'environnement, de l'emplacement	Evaluation basé sur des analyses, qui conduisent à des données périmées et une sensiblité fausse	Etre sensibiliser par la situation en temps réel

Agenda

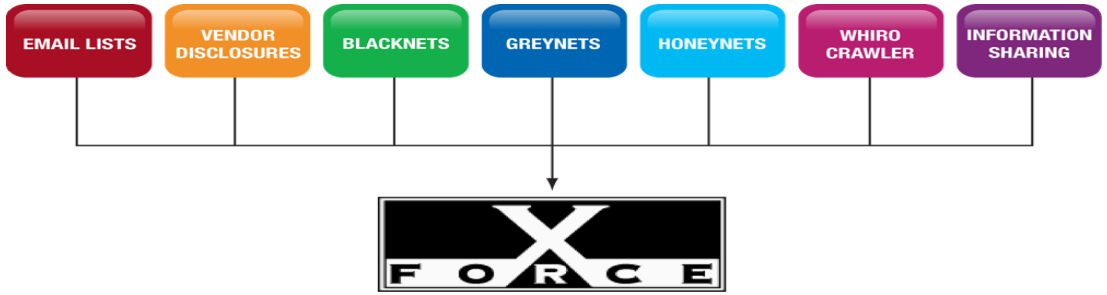
- La vision d'IBM de la sécurité informatique
- Le Cadre de Référence Sécurité
- Les offres Sécurité d'IBM
  - Gestion des Identités et des Accès
  - Protection des applications et des données
  - Protection des postes
  - Protection des infrastructures techniques
  - Supervision de l'activité de sécurité

Evolution des technologies de protection des réseaux

	Firewall	Détection d'intrusion	Prévention d'intrusion
Présentation	Bloque ou autorise le trafic en fonction des caractéristiques de la source et de la destination (adresse/ Port)	Inspecte le flux au niveau des packets et alerte dès qu'une activité suspecte est détectée	Inspecte le flux au niveau des packets et bloque toute activité non conforme ou suspecte
Analogie dans la protection physique	Verrou	Système d'alarme	Garde Armé
Limites	**Les firewalls peuvent être détournés**	**Ne protège pas contre les attaques réseau** **Nécessite une surveillance humaine**	**Tout dépend de la qualité des signatures, politiques ou contenu pour détecter et bloquer avec efficacité les menaces les plus récentes.**

Les Technologies de Sécurité intégrées dans les solutions par la X-FORCE(R&D)

- Moteur d'analyse protocolaire (PAM)
- Virtual Patch: Correctif virtuel avant application du correctif logiciel
- Client-Side application Protection : Protection contre les applications courantes de l'utilisateur final (ex: fichier pdf ou navigateur web)
- Sécurité des applications web : Protection des applications web, web 2.0 et bases de données / Filtrage des accès
- Détection et blocage du trafic malicieux par l'inspection profonde des paquets
- Data Security : Recherche et identification des informations personnelles identifiables et autres informations confidentielles non chiffrées (ex: carte de Sécurité Sociale ou CB)
- Application control : Blocage des applications non autorisées (ex: Skype / P2P)
- Base de signatures référencées



IBM Virtual Patch® technology

- *Shielding a vulnerability from exploitation independent of a software patch*
- *Enables a responsible patch management process that can be adhered to without fear of a breach*
- *IBM is a MAPP (Microsoft Active Protections Program) partner*

At the end of 2009, 53% of all vulnerabilities disclosed during the year had no vendor-supplied patches available to remedy the vulnerability

Matériels IDPS

- Surveillance du trafic réseau
- Inspection en profondeur des paquets (capacité de traitement de 200 Mbps à 20 Gbps)
- Détection, prévention, alertes, concernant les tentatives d'intrusions
- 3 modes de configuration possibles:
  1. Protection passive: Détection des tentatives d'intrusions
  2. Protection potentielle: Cartographie du flux à bloquer)
  3. Protection active: Blocage du flux intrusif

Next-Generation Network IPS: GX7 Model Overview

GX7800

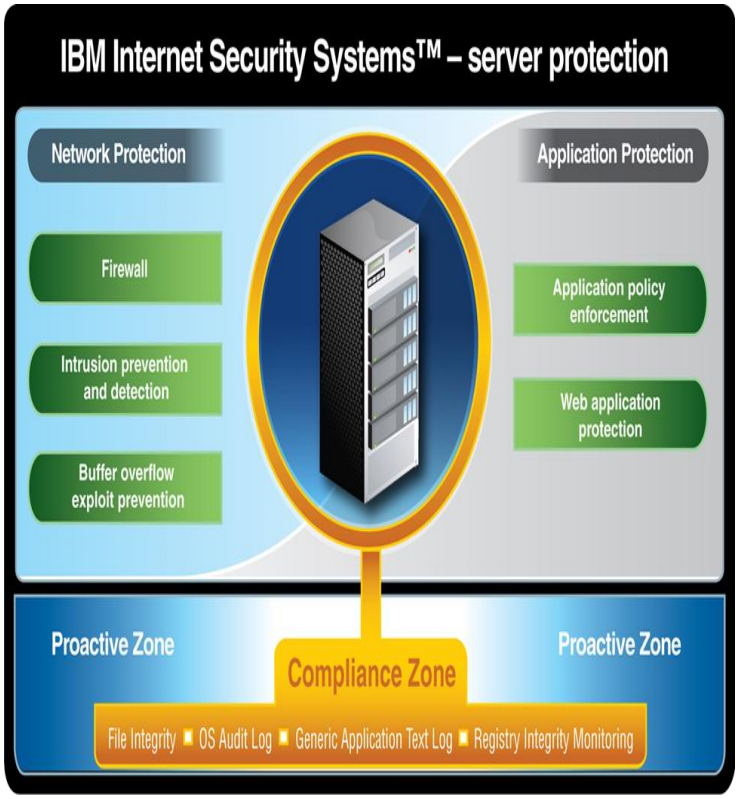
- 8 Ports (4 segments)
- 10G SFP+ (SR,LR)
- 1G SFP (TX,SX,LX)

GX7412

- 16 Ports (8 segments)
  - 4 Ports 1/10G
  - 12 Ports 1G only
- 10G SFP+ (SR,LR)
- 1G SFP (TX,SX,LX)

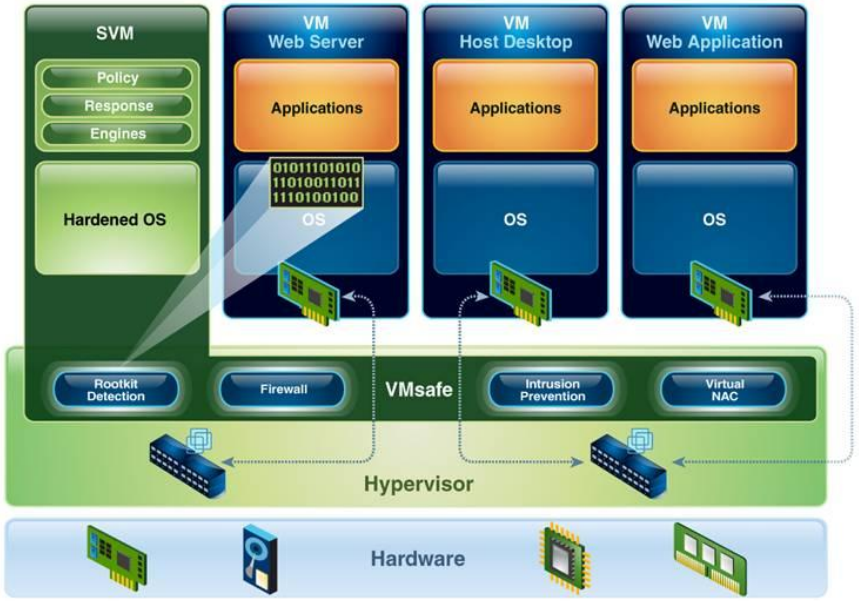
Protection des serveurs: Proventia Server

- Protection des serveurs physiques et des modules virtuels intégrés
- Windows / Linux / zLinux / VMware
- Gestion des accès aux applications et aux fichiers
- Surveillance de l'intégrité des fichiers
- Audit des connexions au Système
- Détection et prévention des intrusions
- Gestions des politiques d'accès aux applications
- Prévention contre l'exploitation de la mémoire tampon
- Protection des données
- Gestion de la conformité



VSP (Virtual Server Protection) Protection des environnements virtuels

- Protection des environnements virtuels (VMware) par le socle central (Hyperviseur)
- Inspection/analyse des flux entre les machines virtuelles
- Détection et blocage des attaques « Rootkit »
- Protection des segments de réseaux virtuels
- Utilisation des fonctionnalités du moteur d'analyse protocolaire (PAM)
- Module IPS embarqué
- Audit des accès à l'infrastructure virtuelle
- Gestion de la conformité

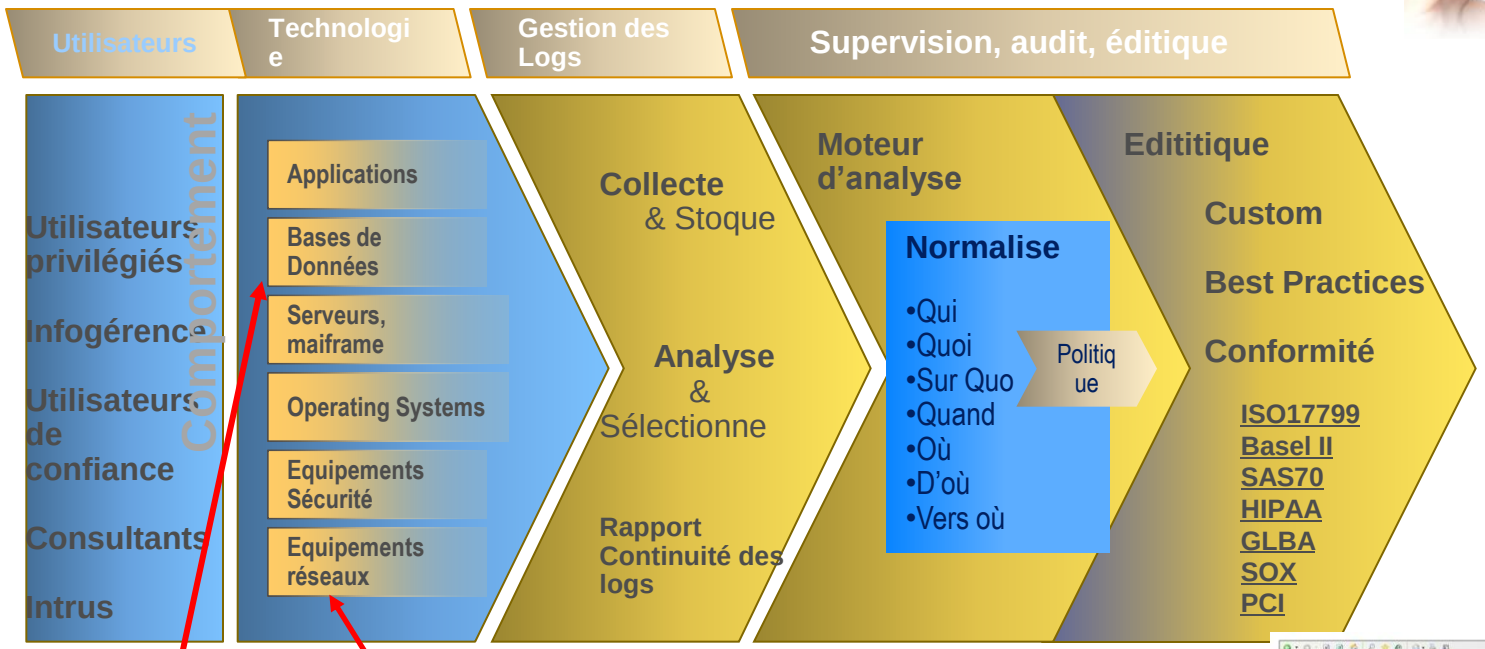


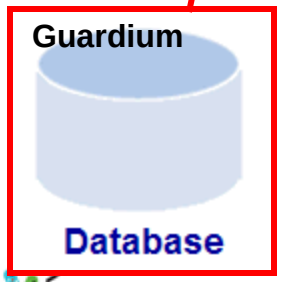
Agenda

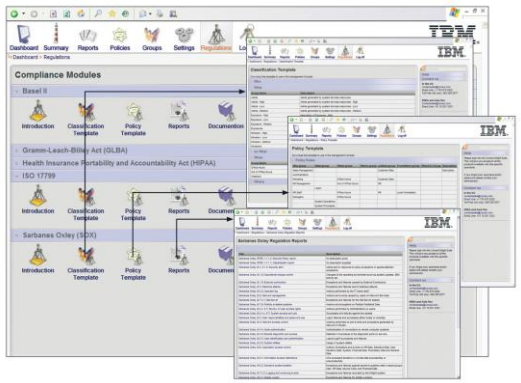
- La vision d'IBM de la sécurité informatique
- Le Cadre de Référence Sécurité
- Les offres Sécurité d'IBM
  - Gestion des Identités et des Accès
  - Protection des applications et des données
  - Protection des postes
  - Protection des infrastructures techniques
  - Supervision de l'activité de sécurité

Supervision de l'activité de sécurité
TSIEM + Supervision de Guardium

Les 7 W + qui a fait quoi au niveau du système et de la base de données et des flux entrants







Merci
Questions ?