IBM SolutionsConnect 2013

L'IBM TechSoftware nouvelle génération

28, 29 et 30 août

IBM Client Center Paris

#solconnect13

Transformez vos opportunités en succès

IBM

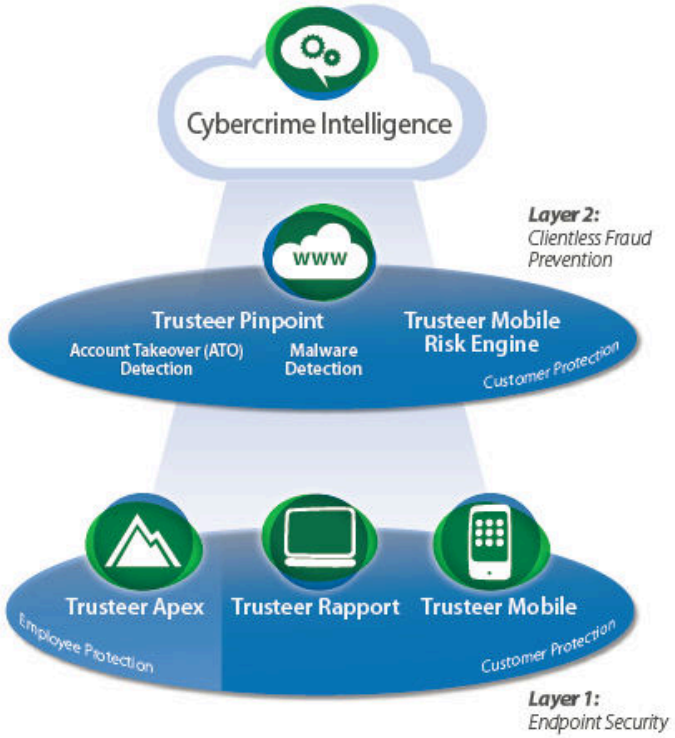
La sécurité du Cloud...
un brin de fraicheur dans les nuages ?

Serge RICHARD - CISSP®
Security Solution Architect – IBM Security Systems

IBM SolutionsConnect 2013

L'IBM TechSoftware nouvelle génération

« L'expertise et la technologie de Trusteer dans la défense du terminal de l'entreprise et la prévention des logiciels malveillants aideront nos clients à travers toutes les industries face aux menaces en constante évolution auxquels ils sont confrontés » Brendan Hannigan, directeur général, division Security Systems d'IBM.



Trusteer Cybercrime Intelligence

Global threat intelligence and fraudster database

Trusteer Pinpoint

Account Takeover (ATO) Detection

Correlation of multiple fraud risk indicators for conclusive account takeover and mobile risk detection

Malware Detection

Clientless detection of Man-in-the-Browser malware infected endpoints

Trusteer Mobile Risk Engine

Detects mobile and cross-channel fraud risk via web-based services and the included mobile client components

Trusteer Apex

Zero-day exploits and data exfiltration prevention for employees' endpoints

Trusteer Rapport

Prevention and remediation of malware and phishing threats on PCs and Macs

Trusteer Mobile

Embedded security library for native mobile apps, dedicated secure mobile browser, out-of-band authentication

Agenda

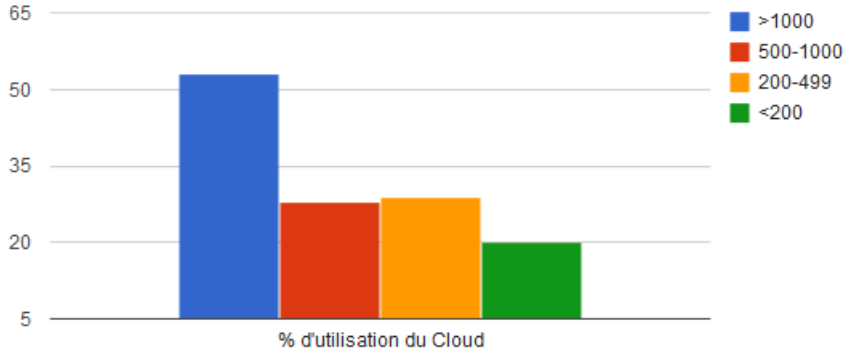
- Point de vue des utilisateurs
- Etat des lieux sur la sécurité des infrastructures CLOUD
- L'approche IBM pour la sécurité des infrastructures CLOUD
- Les offres logicielles et de services IBM

Agenda

- Point de vue des utilisateurs
- Etat des lieux sur la sécurité des infra
- L'approche IBM pour la sécurité des
- Les offres logicielles et de services IBM

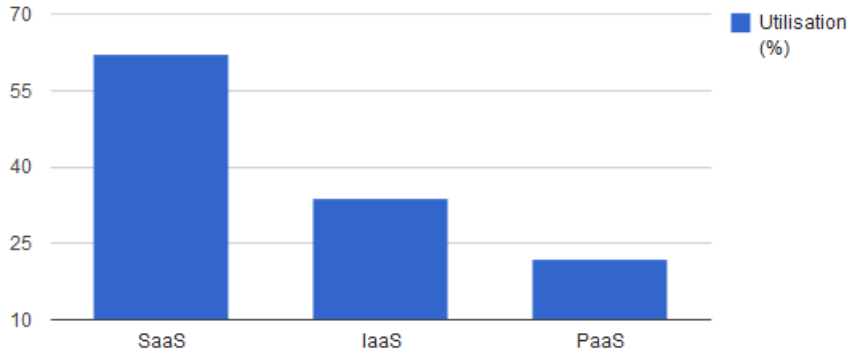
Le Cloud Computing à la française…

Niveau d'utilisation du Cloud selon la taille de l'entreprise



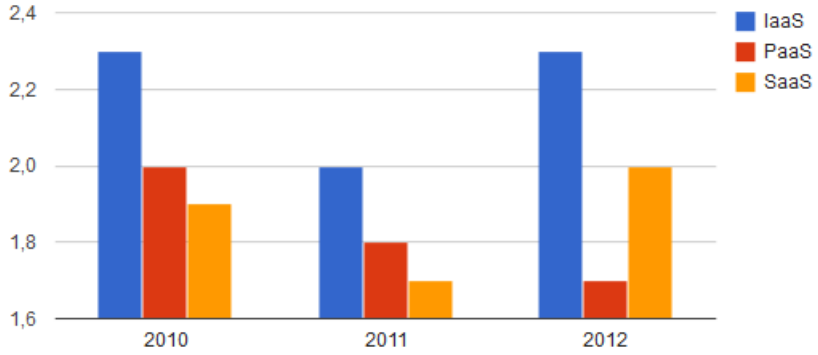
Source PAC - via ZDNet.fr/chiffres-cles

Taux d'utilisation en France par type de Cloud



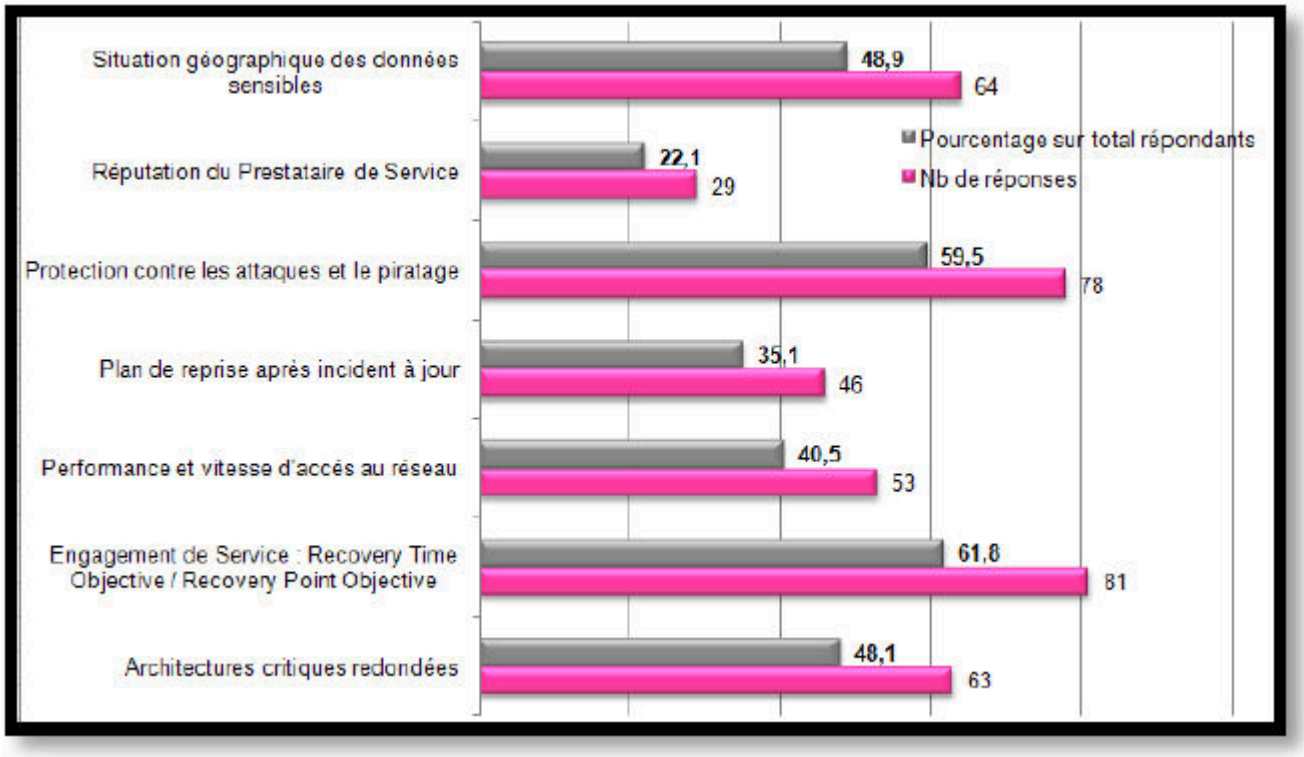
Source PAC - via ZDNet.fr/chiffres-cles

Durée moyenne d'engagement contractuel sur le Cloud



Source Markess - via ZDNet.fr/chiffres-cles

Le CLOUD fait toujours peur...



http://www.t-systems.fr/presse-analystes/centre-de-presse/990154_1/blobBinary/20-09-12_Barom%25C3%25A8tre-T-Systems-ps.pdf

Et personne n'est là pour nous rassurer…

Forces	Faiblesses
• Permet une plus grande flexibilité (dimensionnement à la demande) ; • Permet un espace de stockage virtuel ; • Accessibilité des données de n'importe quel terminal ; • Permet une réduction des coûts d'investissement ; • Facilite le travail collaboratif ; • Nombreux datacenters à proximité ; • Bénéficie de réseaux THD et de communication de première importance ; • Un réseau d'acteurs du Cloud déjà présent et structuré autour d'associations professionnelles ; • Visibilité nationale et internationale des entreprises (Salons, congrès, expositions à Paris).	• Nécessite une profonde refonte du système informatique ; • L'accessibilité des données dépend de celle d'internet ; • Opacité sur la localisation et donc la sécurité des données ; • Complexité contractuelle avec le fournisseur de Cloud ; • Nombreuses start-up fragiles ; • Retard dans le développement de la filière par rapport aux Etats-Unis et à l'Asie.
Opportunités	**Menaces**
• Un levier d'action pour le Green IT ; • Un changement de modèle économique et de relation client/fournisseur ; • L'informatique comme un moyen d'innovation pour les entreprises ; • Utilisation facilitée du calcul intensif pour de nouveaux axes de R&D ; • Un levier de modernisation pour l'Etat ; • Recentrer les investissements sur les tâches à valeur ajoutée ; • Volonté politique de mettre l'accent sur le Cloud.	• Remise en question du rôle des DSI ; • Perte de contrôle de son infrastructure et dépendance vis-à-vis du fournisseur de Cloud ; • Inadéquation entre l'activité de l'entreprise et son passage au Cloud ; • Flou sur la localisation de ses données et leur sécurité ; • Marché hyperactif et hyperconcurrentiel ; • Cadre juridiques et réglementaires ; • Saturation du nombre de datacenters en Ile-de-France (approvisionnement en électricité).

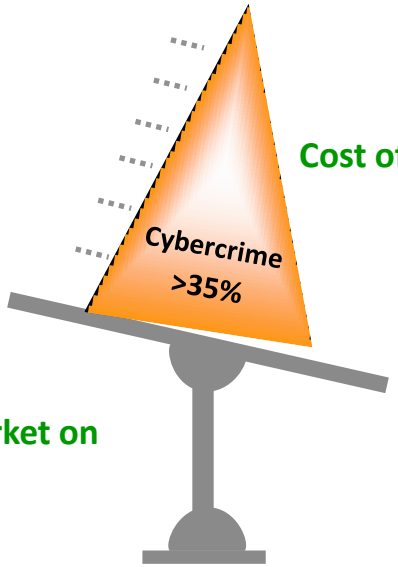
http://direccte.gouv.fr/IMG/pdf/cloud_computing_final.pdf

Beaucoup de personnes ont un avis sur la question…

Agenda

- Point de vue des utilisateurs
- Etat des lieux sur la sécurité des infrastructures CLOUD
- L'approche IBM pour la sécurité des infrastructur
- Les offres logicielles et de services IBM

L'avènement du Criminel 2.0…



Cost of Global Cyber Crime

$388B

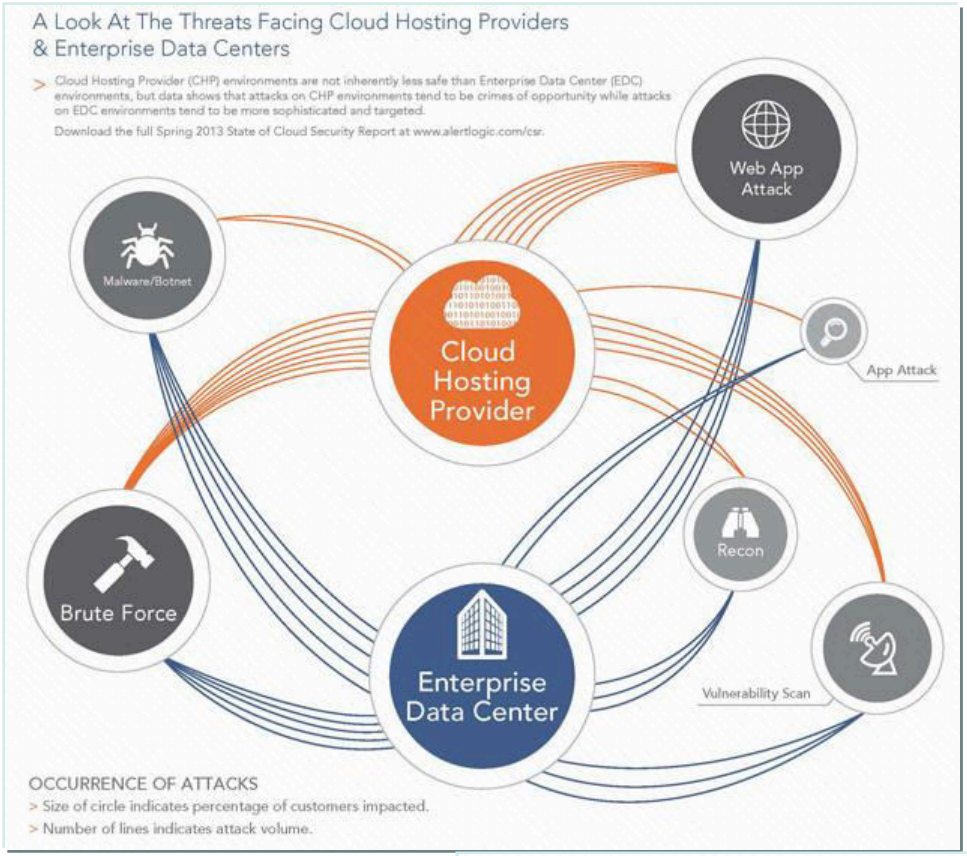
Global Black Market on Drugs

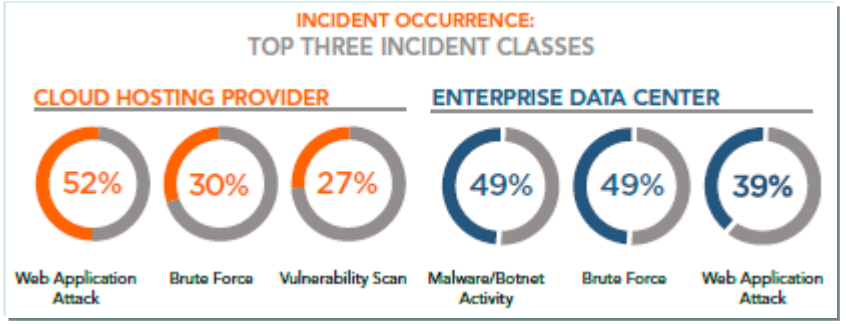
$288B

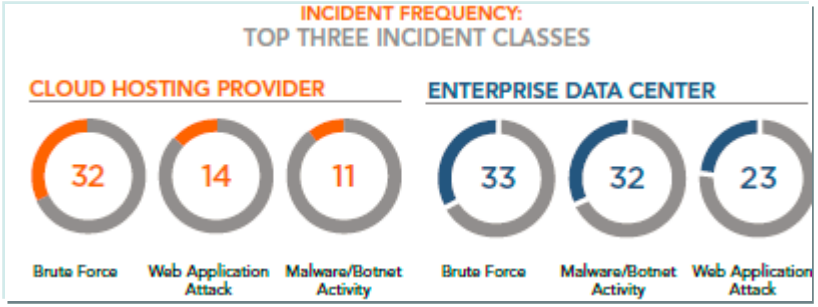
http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02

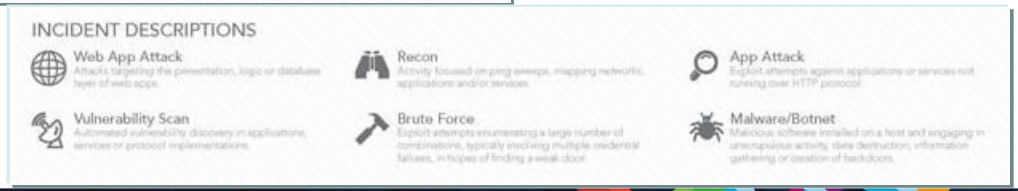
"You know you can do this just as easily online."

La sécurité du Cloud en 2012 (source AlertLogic – http://www.alertlogic.com)



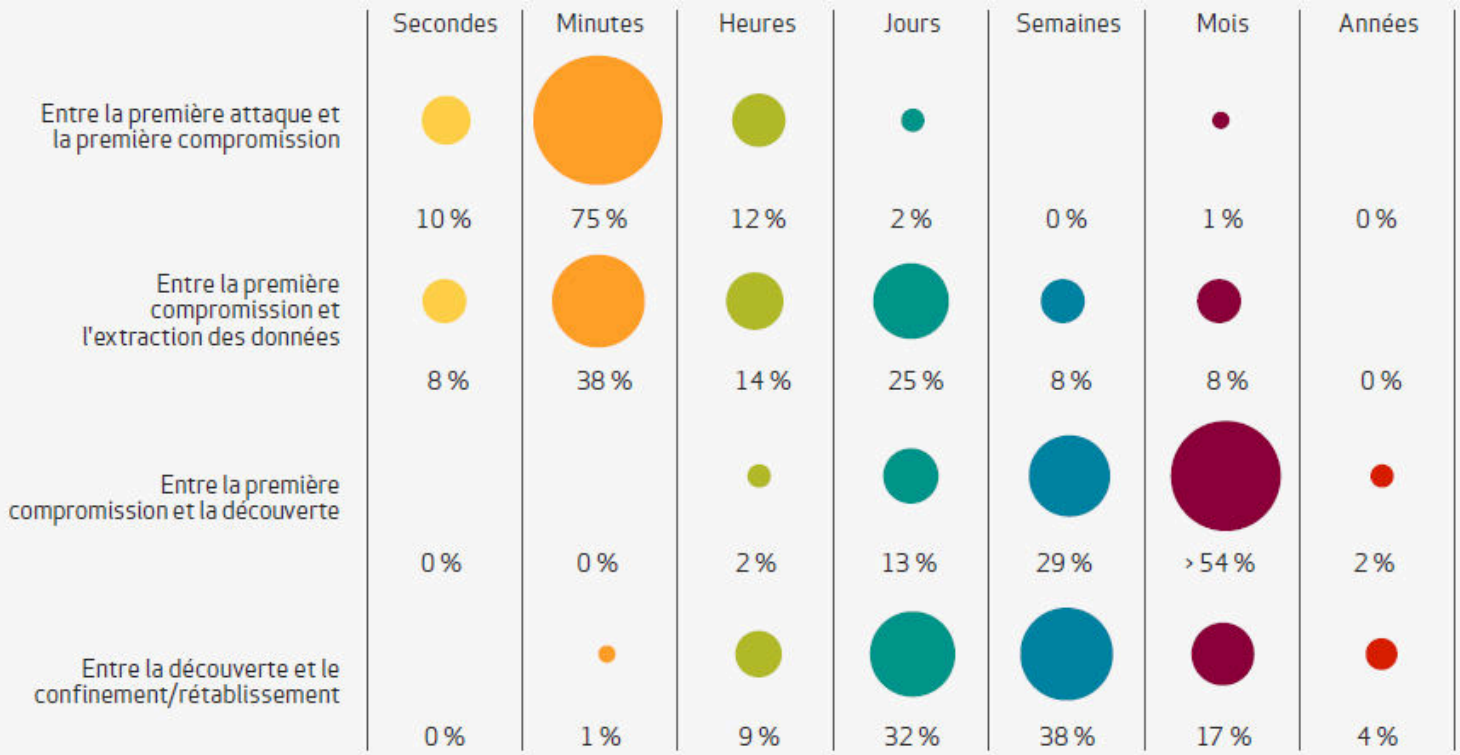






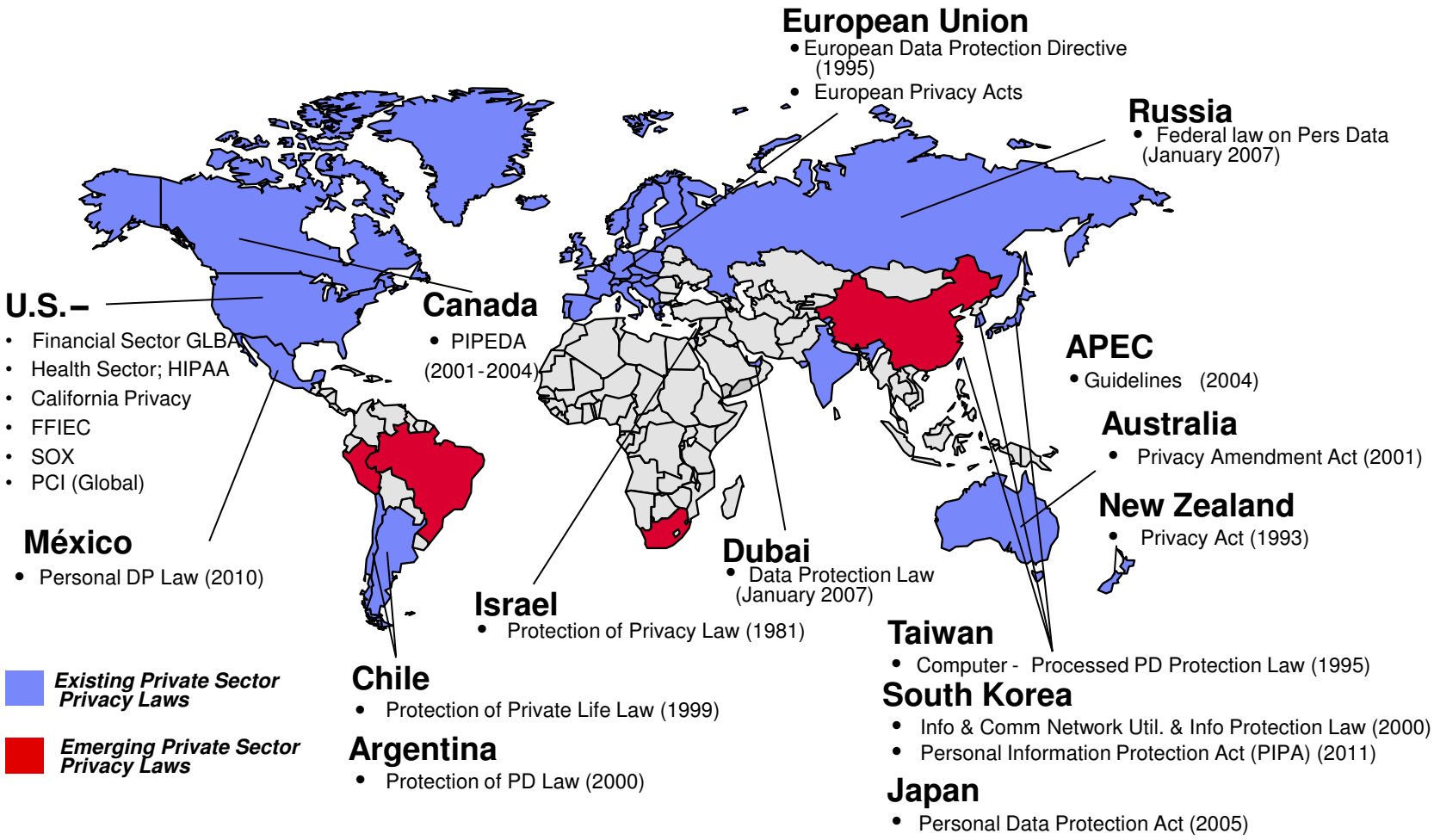
Et comment sont gérer les attaques sur votre infrastructure CLOUD ?

Figure 40. Durée des événements par pourcentage de compromissions



http://www.verizonenterprise.com/resources/reports/rp_Rapport_d_enquete_2012_Sur_Les_Compromissions_De_Donnees_fr_xg.pdf

Contraintes de réglementation et de conformité inhérentes à chaque pays



Agenda

- Point de vue des utilisateurs
- Etat des lieux sur la sécurité des infrastructures CLC
- L'approche IBM pour la sécurité des infrastructures CLOUD
- Les offres logicielles et de services IBM

Le CLOUD modifie notre manière de penser la sécurité.

Un environnement Cloud se caractérise par des accès étendus, des changements de responsabilités, une transformation des capacités de contrôle et l'accroissement de la vitesse de provisionnement des ressources informatiques **avec un impact considérable sur tous les aspects de la sécurité.**

Cloud privé

Infrastructure Cloud, implantée localement ou non, exploitée exclusivement par une entreprise, et administrée par cette entreprise ou par un tiers.

Informatique hybride

Informatique traditionnelle et clouds (publics et/ou privés) restant distincts, mais liés mutuellement par une technologie assurant la portabilité des données et des applications.

Cloud public

Disponible auprès du grand public ou d'un groupe industriel étendu, et contrôlé par une entreprise commercialisant des services Cloud.

Évolutions en matière de sécurité et de confidentialité

- *Responsabilité du client concernant l'infrastructure.*
- *Personnalisation accrue des contrôles de sécurité.*
- *Bonne visibilité sur les opérations courantes.*
- *Facilité d'accès aux journaux et aux règles.*
- *Les applications et les données sont protégées par un pare-feu.*

- *Responsabilité du fournisseur concernant l'infrastructure.*
- *Moins de personnalisation des contrôles de sécurité.*
- *Aucune visibilité sur les opérations courantes.*
- *Difficultés d'accès aux journaux et aux règles.*
- *Les applications et les données sont accessibles de manière publique.*

Minimiser les risques du Cloud nécessite une approche stratégique

Définir une stratégie Cloud en y intégrant la sécurité

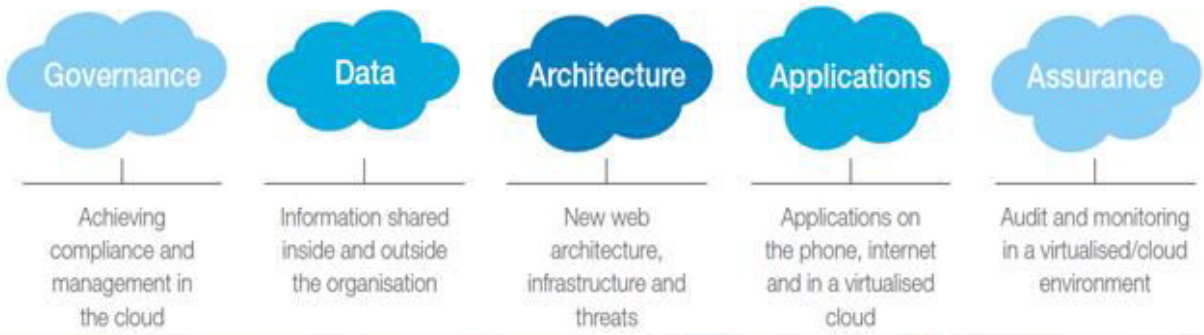
- Identifier les différentes charges (workloads) et leurs modes d'interaction.
- Quels sont les modèles appropriés en fonction des exigences de sécurité et de confiance, et les systèmes auxquels ils doivent s'interfacer ?

Identifier les mesures de sécurité nécessaires

- L'utilisation d'une méthodologie telle que IBM Security Framework permet d'évaluer les besoins en matière de gouvernance, d'architecture, d'applications et d'assurance.

Mettre en œuvre une approche de sécurité pour l'environnement Cloud

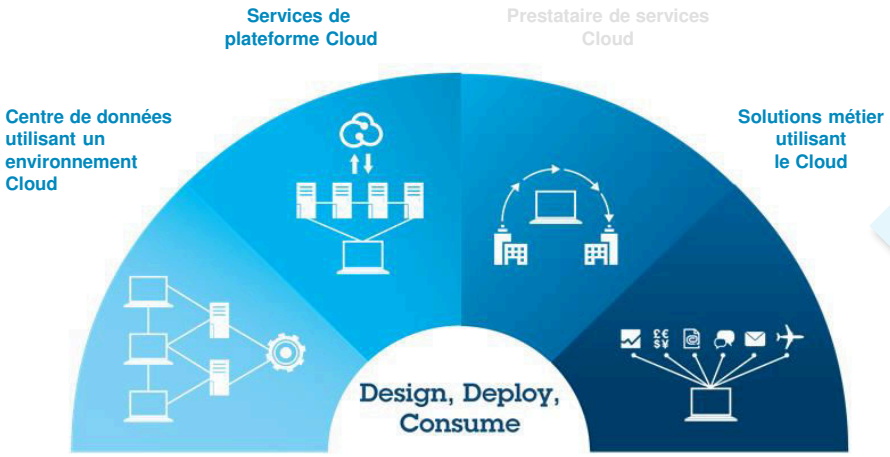
- Définir l'ensemble initial de dispositions d'assurance à adopter.
- Évaluer le niveau de respect des besoins en sécurité des applications, de l'infrastructure et des autres éléments, ainsi que les mesures de sécurité opérationnelle mises en place.



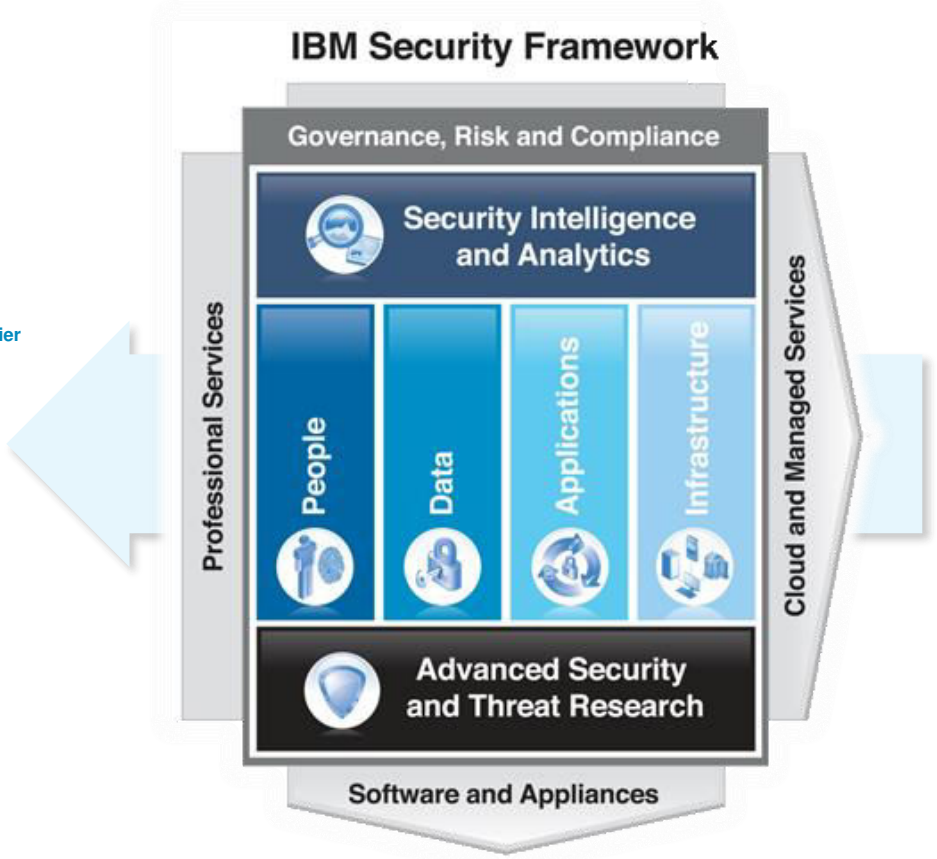
L'expérience étendue et les capacités d'IBM en matière de sécurité s'appliquent à tous les profils d'adoption du Cloud

IBM Cloud Security

Chaque configuration nécessite une réponse spécifique



Les contrôles de sécurité sont conçus en fonction des différents besoins d'un environnement Cloud - le défi consiste à assurer l'intégration, la coexistence et l'identification de la solution la plus efficace pour une charge de travail donnée.



Chaque profil se caractérise par son propre éventail d'approches prioritaires de sécurité

Infrastructure as a Service (IaaS) : Réduire les dépenses et la complexité informatiques grâce aux centres de données Cloud.

Platform-as-a-Service (PaaS) : Réduire le délai de mise sur le marché grâce aux services de plateforme Cloud

Créer des **business models innovants** en devenant un prestataire de services Cloud.

Software as a Service (SaaS) : Accéder immédiatement à des solutions métier fonctionnant dans l'environnement Cloud.

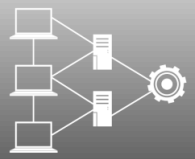
Centre de données utilisant un environnement Cloud

Services externalisés intégrés, automatisation, provisionnement, libre-service

Axes essentiels de la sécurité :

Infrastructure et identités

- Gérer les identités au sein des centres de données.
- Sécuriser les machines virtuelles.
- Appliquer des correctifs logiciels aux images par défaut.
- Surveiller les journaux de l'ensemble des ressources.
- Isolation des réseaux.



Services de plateforme Cloud

Infrastructure informatique préassemblée et pré-intégrée en fonction de besoins spécifiques à des applications

Axes essentiels de la sécurité :

Applications et données

- Sécuriser les bases de données partagées.
- Chiffrer les informations privées.
- Construire des applications sécurisées.
- Conserver des informations d'audit.
- Intégrer la sécurité existante.

Prestataire de services Cloud

Une plateforme évoluée pour créer, gérer et monétiser des services Cloud

Axes essentiels de la sécurité :

Données et conformité

- Isoler les locataires du Cloud.
- Politique et réglementation.
- Gérer les activités de sécurité.
- Construire des centres de données conformes.
- Mettre en place des capacités de sauvegarde et de résilience.

Solutions métier utilisant le Cloud

Fonctionnalités offertes aux consommateurs pour utiliser les applications d'un fournisseur

Axes essentiels de la sécurité :

Conformité et gouvernance

- Renforcer les applications exposées.
- Fédérer de manière sécurisée des identités.
- Déployer des processus de contrôle d'accès.
- Chiffre les communications.
- Gérer les règles d'utilisation des applications.

Notre approche de la mise en œuvre d'une démarche de sécurité dans l'environnement Cloud s'adapte à chacune des phases d'un projet ou d'une initiative client.

Concevoir
Établir une stratégie Cloud et un plan de mise en œuvre pour la réaliser.

Déployer
Bâtir des services Cloud, au sein de l'entreprise et/ou en tant que prestataire de services Cloud.

Utiliser
Gérer et optimiser l'utilisation des services Cloud.

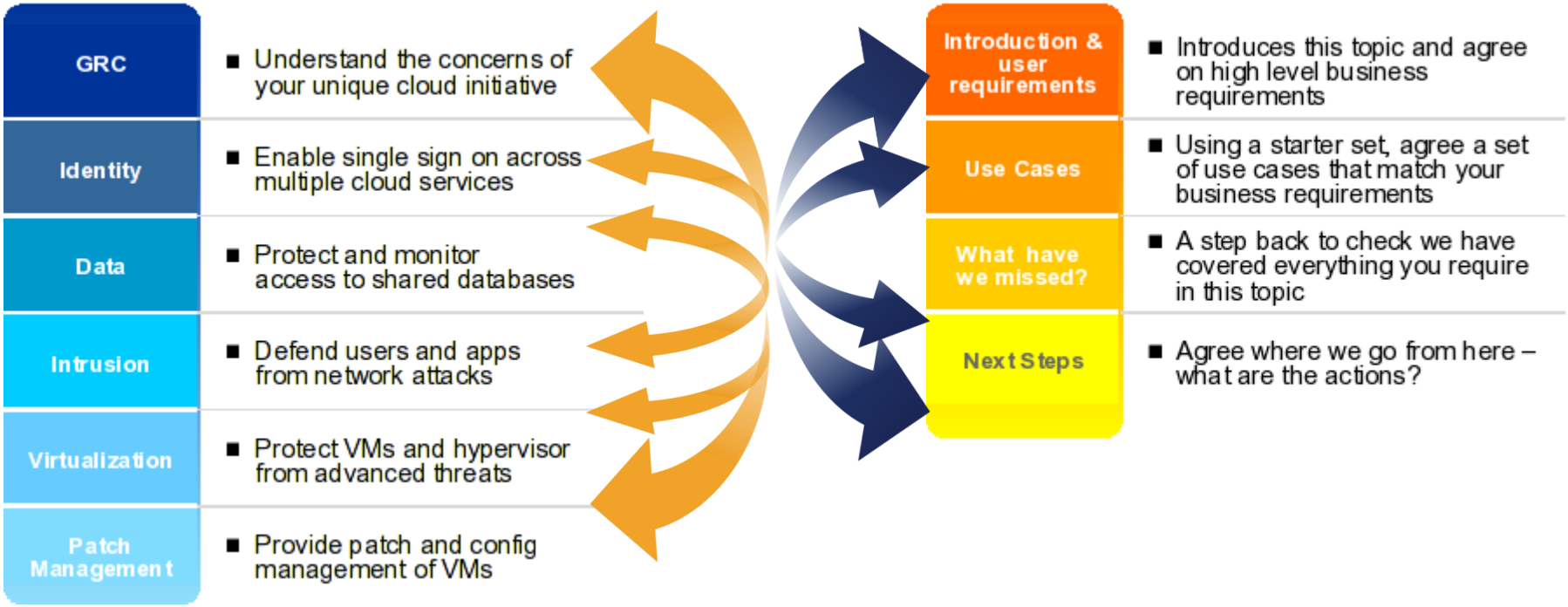
Approche IBM de la sécurité du Cloud	*Sécurité intégrée à la conception*	*Piloté par les charges de travail*	*Axé sur les services*
	L'objectif est d'intégrer la sécurité dans la structure du Cloud.	*Des ressources Cloud sécurisées dotées de fonctionnalités et de produits innovants.*	*Gouvernance du Cloud englobant des activités permanentes et un workflow de sécurité.*
Exemples de fonctionnalités de sécurité	▪ Plan d'action de la sécurité d'un environnement Cloud. ▪ Développement sécurisé. ▪ Protection des menaces affectant les réseaux. ▪ Sécurité des serveurs. ▪ Sécurité des bases de données.	▪ Sécurité des applications. ▪ Sécurité de la virtualisation. ▪ Protection des points d'extrémité. ▪ Gestion des configurations et des correctifs.	▪ Gestion des identités et des accès. ▪ Communications Cloud sécurisées. ▪ Services de sécurité externalisés.

Pour vous permettre de démarrer la démarche, nous avons développé un éventail complet de contrôles de sécurité pour le Cloud

Les voies d'accès à la sécurité du Cloud

			Concevoir	Déployer	Utiliser
Sécurité Intelligente	▪ Visibilité totale des environnements virtuels et Cloud.	Plateforme IBM QRadar Security Intelligence (SIEM, Risk Manager)	X	X	X
Individus	▪ Permettre la signature unique pour une multiplicité de services Cloud.	IBM Federated Identity Manager Business GW			X
Données	▪ Protéger et surveiller les accès aux bases de données partagées.	IBM® InfoSphere Guardium	X	X	
Applications	▪ Analyser les applications web déployées dans le Cloud.	IBM Rational AppScan Suite		X	
Infrastructure	▪ Protéger les utilisateurs et les applications des attaques réseau.	IBM Security Network Intrusion Prevention System	X		
	▪ Protéger les machines virtuelles et l'hyperviseur vis-à-vis des menaces évoluées.	IBM Virtual Server Protection for VMware	X	X	
	▪ Assurer la gestion des correctifs logiciels et des configurations sur les machines virtuelles.	IBM Tivoli Endpoint Manager for Security and Compliance		X	X
Services	▪ Connaître les enjeux de votre initiative spécifique en matière de Cloud.	IBM Cloud Security Roadmap Service	X		

Mise en place d'un atelier sécurité architecture CLOUD

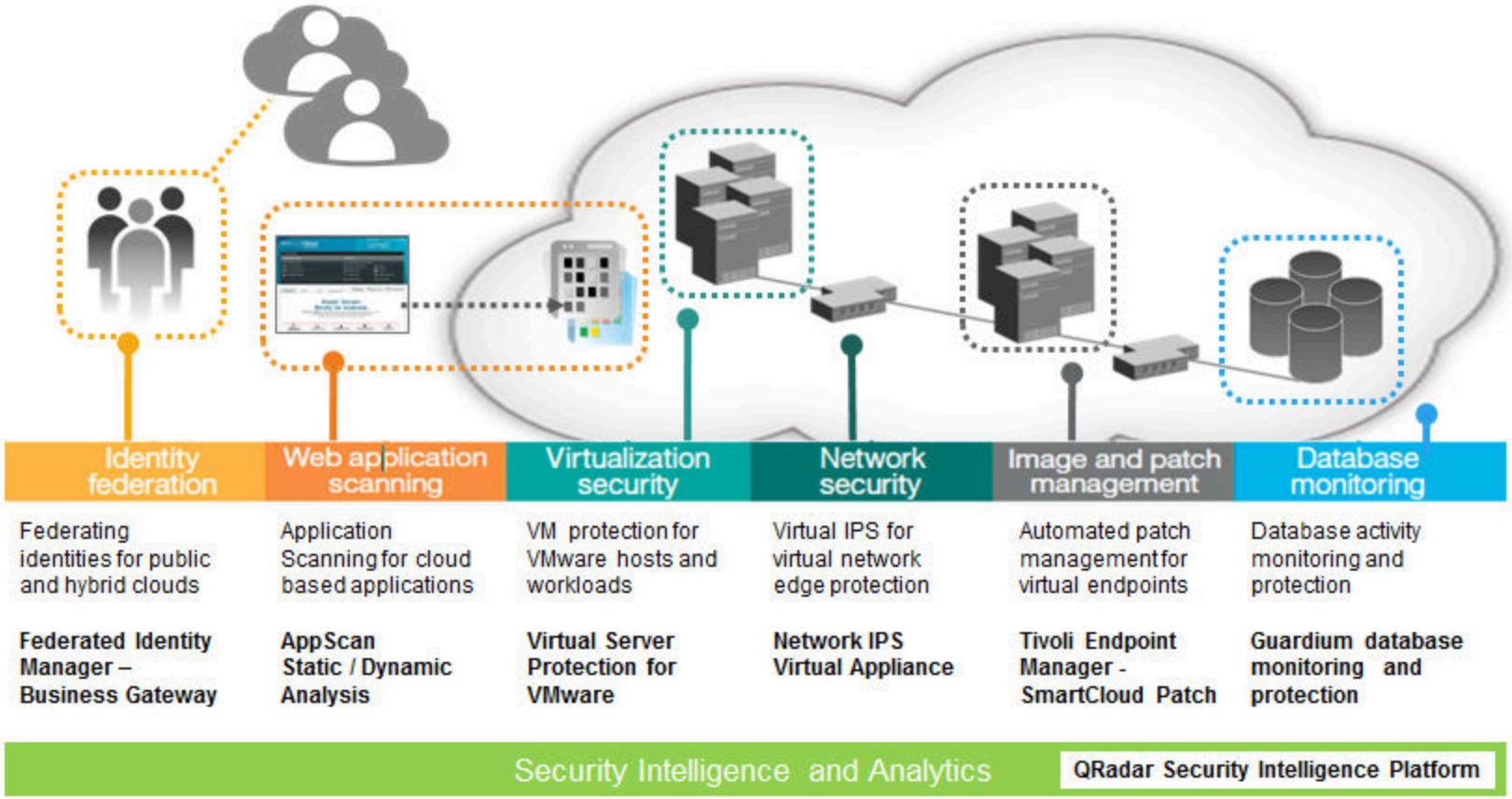


Agenda

- Point de vue des utilisateurs
- Etat des lieux sur la sécurité des infrastructures CLOUD
- L'approche IBM pour la sécurité des infrastructures CLOUD
- Les offres logicielles et de services IBM

L'approche solution IBM Cloud Security permet de garder le contrôle et la visibilité

Une approche solution logicielle globale

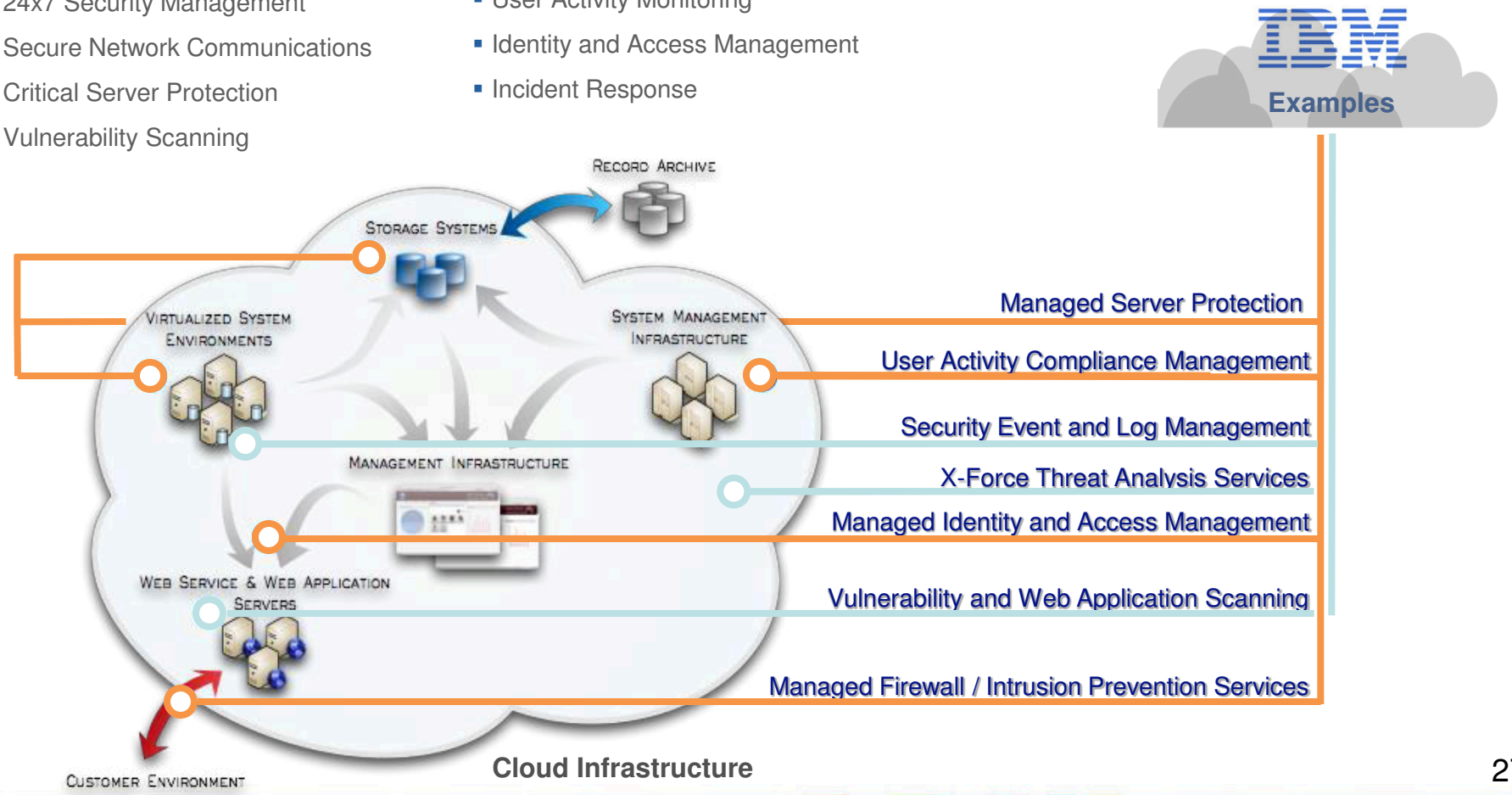


Smart Cloud Security Services **fournis *PAR*** le Cloud :

Une approche solution service globale

Key areas where MSS can assist:

- 24x7 Security Management
- Secure Network Communications
- Critical Server Protection
- Vulnerability Scanning
- User Activity Monitoring
- Identity and Access Management
- Incident Response



Smart Cloud Security Services **fournis *POUR*** le Cloud :

Professional Service

Cloud Security Strategy Roadmap

Comprendre les besoins du Cloud en terme de conformité et de gouvernance sécurité

Professional Service

Cloud Security Assessment

Aider les fournisseurs de Cloud (public / privé / hybride) à évaluer la sécurité avec les meilleures pratiques

Managed Service

Managed Intrusion Prevention Services

Assurer une protection contre les menaces dans le but d'atténuer les attaques sur l'environnement Cloud

Services de consulting

Evaluer ou sécuriser le Cloud

Pour hébergeurs ou entreprises

Professional Service

Penetration Testing

Valider la sécurité de l'architecture Cloud au travers d'une supervision active et des tests de pénétration

Professional Service

Identity and Access Management

Évaluer la stratégie d'authentification d'un environnement Cloud et propose un plan d'optimisation de l'approche par rapport aux objectifs de l'entreprise

Professional Service

Application Security Assessment

Évaluer la sécurité des applications basées dans le Cloud : soit par une analyse dynamique, soit par une revue de code

Les solutions IBM Cloud Security apportent aux clients les moyens de restaurer leurs capacités de visibilité et de contrôle

Couverture de bout en bout permettant de sécuriser les Clouds privés, hybrides et publics.

IBM est le seul fournisseur proposant des produits, des services et une expertise permettant de sécuriser les aspects critiques du Cloud - englobant ainsi **les utilisateurs, les données, les applications** et **les infrastructures virtualisées.**

- **Sécurité hautement performante** dans tous les secteurs du Cloud.
- **Visibilité** sur la sécurité des environnements Cloud.
- **Sécuriser l'accès** aux applications Cloud.
- **Protection des données** dynamiques et statiques.
- Solutions de **gestion des menaces et des vulnérabilités** pour les applications et les infrastructures.
- **Services** spécifiquement conçus pour sécuriser le Cloud.

**La protection
la plus performante
pour le Cloud Computing**

IBM poursuit ses activités pour rechercher, tester et documenter des approches encore plus efficaces en matière de sécurité des environnements Cloud

IBM Research

Des actions spécifiquement focalisées sur la sécurité du Cloud

IBM® X-FORCE

Une équipe chargée d'activités de contre-renseignement et d'information du public

Communautés de clients

Des retours d'informations concrets provenant de clients ayant adopté le Cloud

Participation aux activités sur les normes ouvertes

Normes ouvertes centrées sur le client et interopérabilité

IBM Institute for Advanced Security

Collaboration entre les universités, l'industrie, l'administration publique et la communauté technique IBM.

IBM SolutionsConnect 2013

L'IBM TechSoftware nouvelle génération