sécurité applicative

éléments de sensibilisation

Philippe ENSARGUET
Orange Business Services
Head of IT Architecture Skills Center
IT&L@BS Technical board
philippe.ensarguet@orange-ftgroup.com

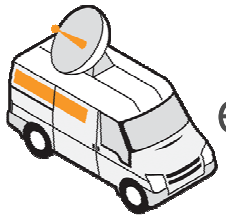
témoignages

exemple 1 : plate-forme eCommerce

- Problèmes fonctionnels
- Spécification de besoins

exemple 2 : application métier de calcul en ligne des retraites

- Problèmes fonctionnels/applicatifs
- Spécification détaillée et conception de l'architecture



exemple 3 : site de vente de vidéo en ligne

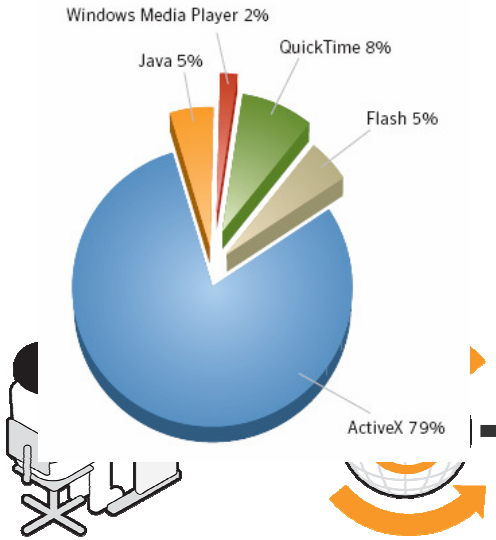
- Problèmes applicatifs
- Implémentation

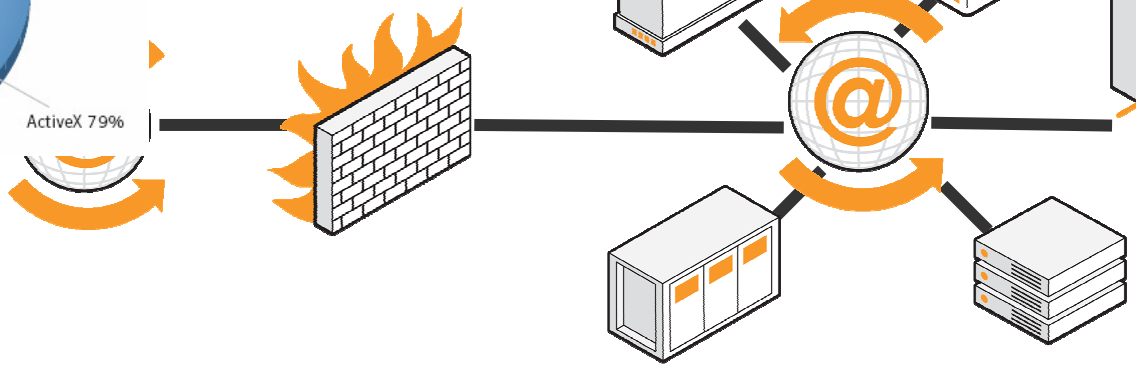
exemple 4 : système de gestion de code

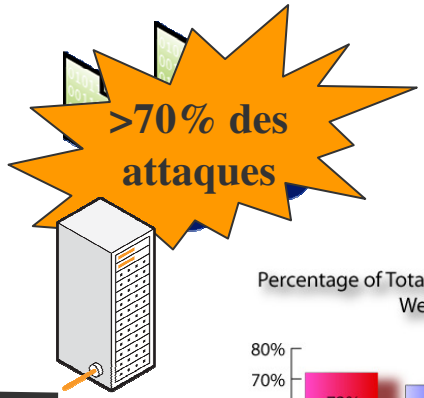
- Pas de référentiel partagé
- Pas de normalité dans la sécurité

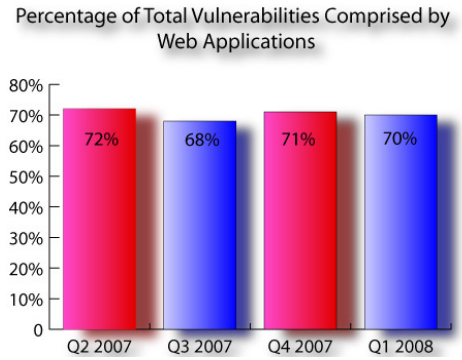
un spectre large

Poste client | Couches transports | Filtrage cloisonnement | Environnement production | Couche applicative









Source : senzic.com

Antivirus
AntiSpyware
Proxy
Firewall
…

Chiffrement

Contrôle d'accès

IPS
IDS
SSO

Sécurité applicative

Business Services orange

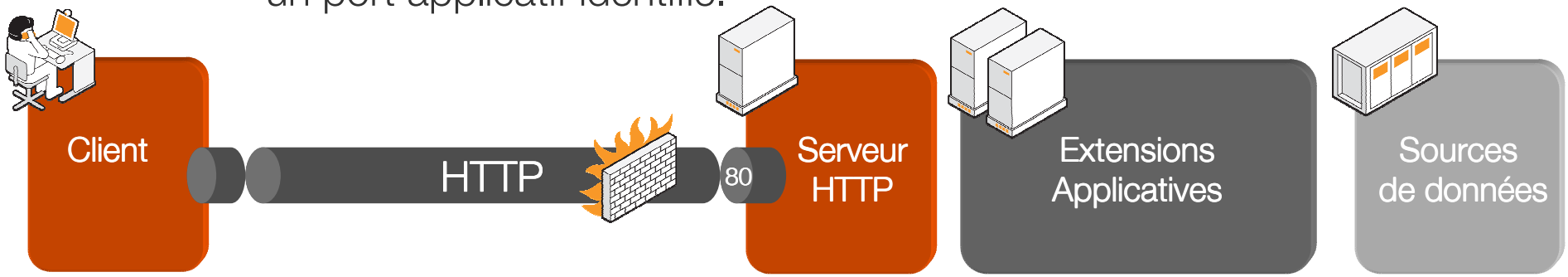
tour d'horizon des vulnérabilités en présence

Source : owasp.org

nous sommes tous concernés !

généralité sur les applications Web

> une application Web c'est…
  - … une relation entre un client et un serveur,
  - … mis en relation par l'infrastructure d'acheminement TCP/IP de l'internet,
  - … dialoguant au travers d'un protocole applicatif de requêtage HTTP sur un port applicatif identifié.



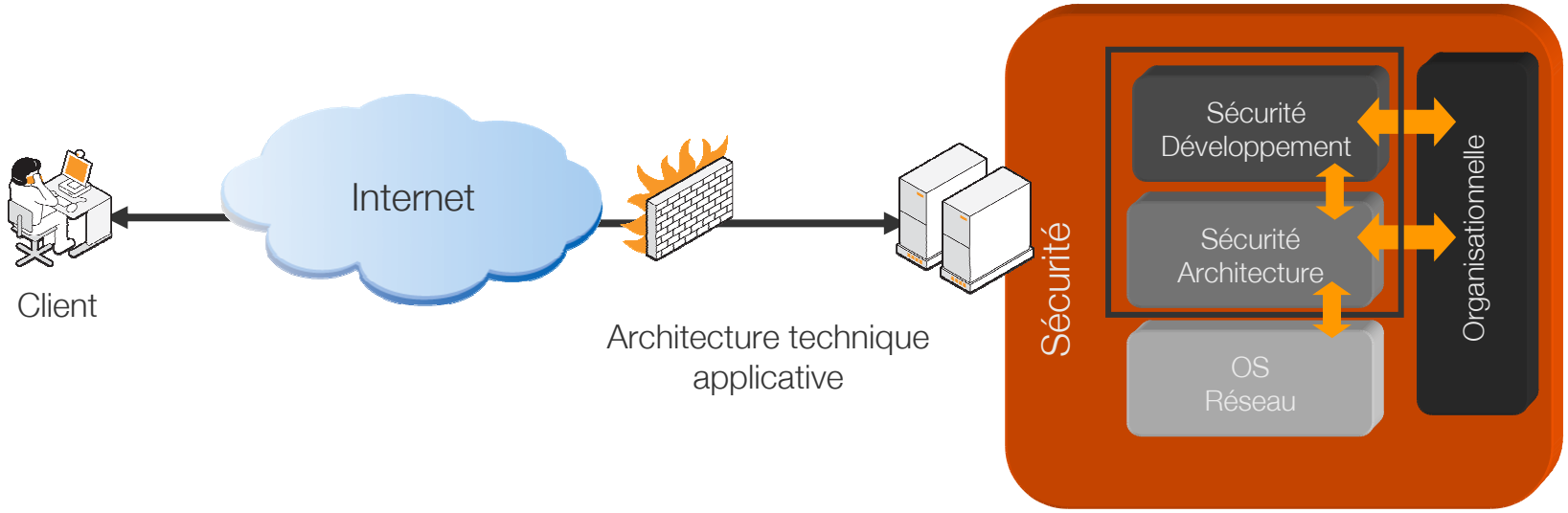
>Apache
>IIS
>…

>SSI
>CGI (Perl, Python, PHP,…)
>Extension HTTP (ISAPI,AAPI, …)
>Server-side Scripting (ASP,JSP, PHP,…)
>Serveurs d'application(Java EE, .Net)

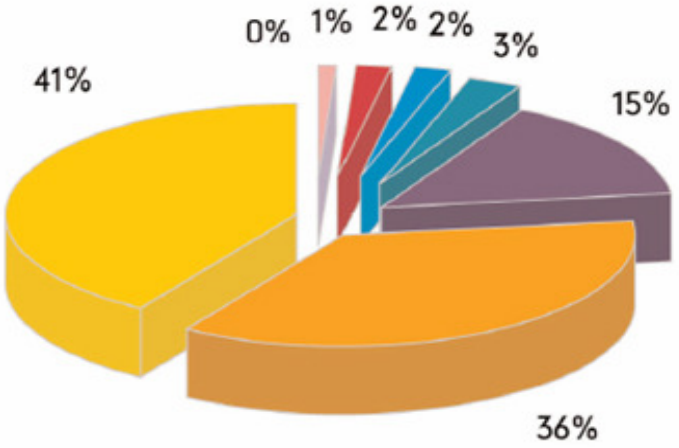
constat : Les applications distribuées sur le web sont incontournables

tendance et évolution de la sécurité

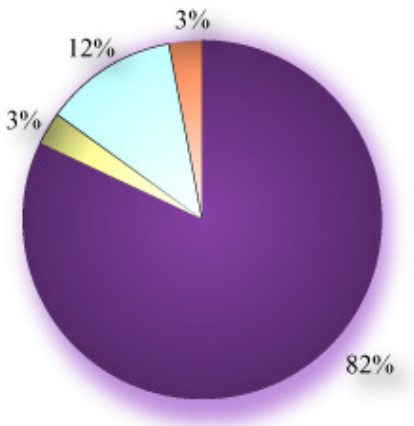
> depuis plus de 15 ans, de nombreuses technologies d'implémentation
  - aucune technologie ne s'est montrée invulnérable !
  - exploitation de failles/vulnérabilités portant une atteinte à l'intégrité, la confidentialité, l'imputabilité et l'accès aux données utilisateurs.

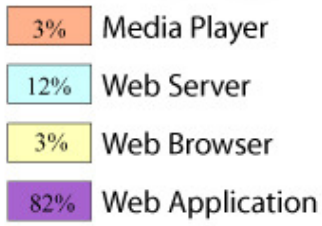


quelques chiffres pour confirmer !



SOURCE: NIST





Source : cenzic.com

évolution des attaques

> depuis quelques années


meilleure prise en compte des recommandations sur la sécurité périmétrique


firewall, cloisonnement, passerelles (reverse proxy…)


serveurs publiques : configurés et minimisés


vulnérabilités corrigées et OS stables (appliances)


attaques plus difficiles à mettre en œuvre au niveau de l'infrastructure

évolution des attaques

- évolution des attaques
  - montée dans les couches du modèle OSI
  - ports applicatifs : HTTP/HTTPS,...
  - à la fois :
    - directement, par les serveurs applicatifs et les applications métiers
    - indirectement, via les postes utilisateurs
- flux autorisés vers les serveurs
  - accès direct aux conteneurs applicatifs
  - flux plus ou moins surveillés
- solutions/produits ayant, par essence, davantage de vulnérabilités
  - délai de mise en place du patch

évolution des attaques

les machines des utilisateurs internes sont :

- moins protégées / plus de fonctionnalités
- connectées / autorisées sur le réseau interne
- accèdent à Internet

> applications métiers propriétaires

- non éprouvées
- peu auditées

> lien direct avec les données métiers

> de nombreuses vulnérabilités !

objectifs de ces attaques

- récupération d'informations confidentielles (identité des utilisateurs, informations bancaires,…)

  atteinte à la confidentialité

- modification du contenu
  - données internes (BDD financière, cliente…)
  - sites Web publiques (façade commerciale)

  atteinte à l'intégrité

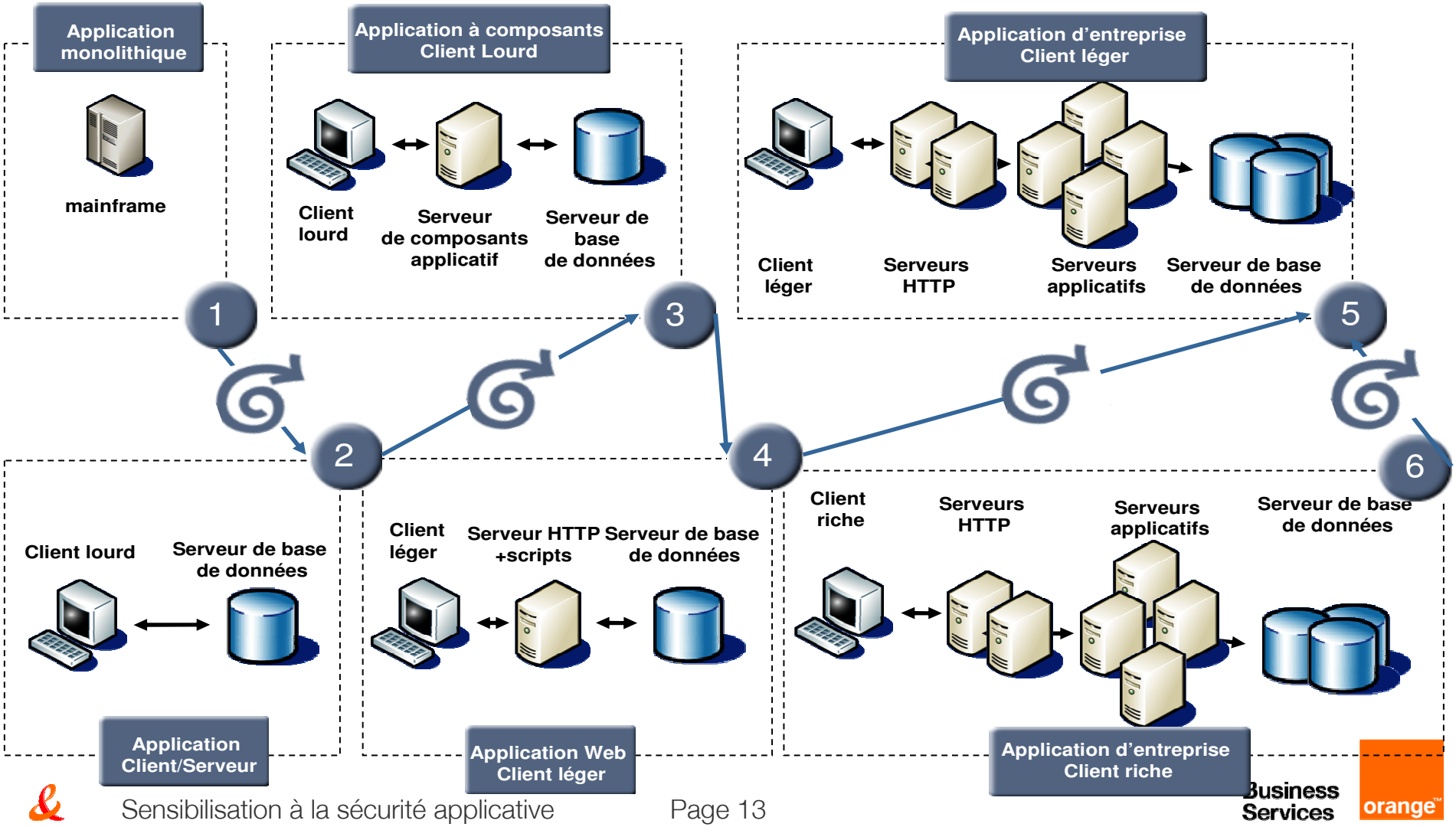
- rendre le service indisponible (Déni de Service – DoS)
  - temporaire
  - permanente

  atteinte à la disponibilité

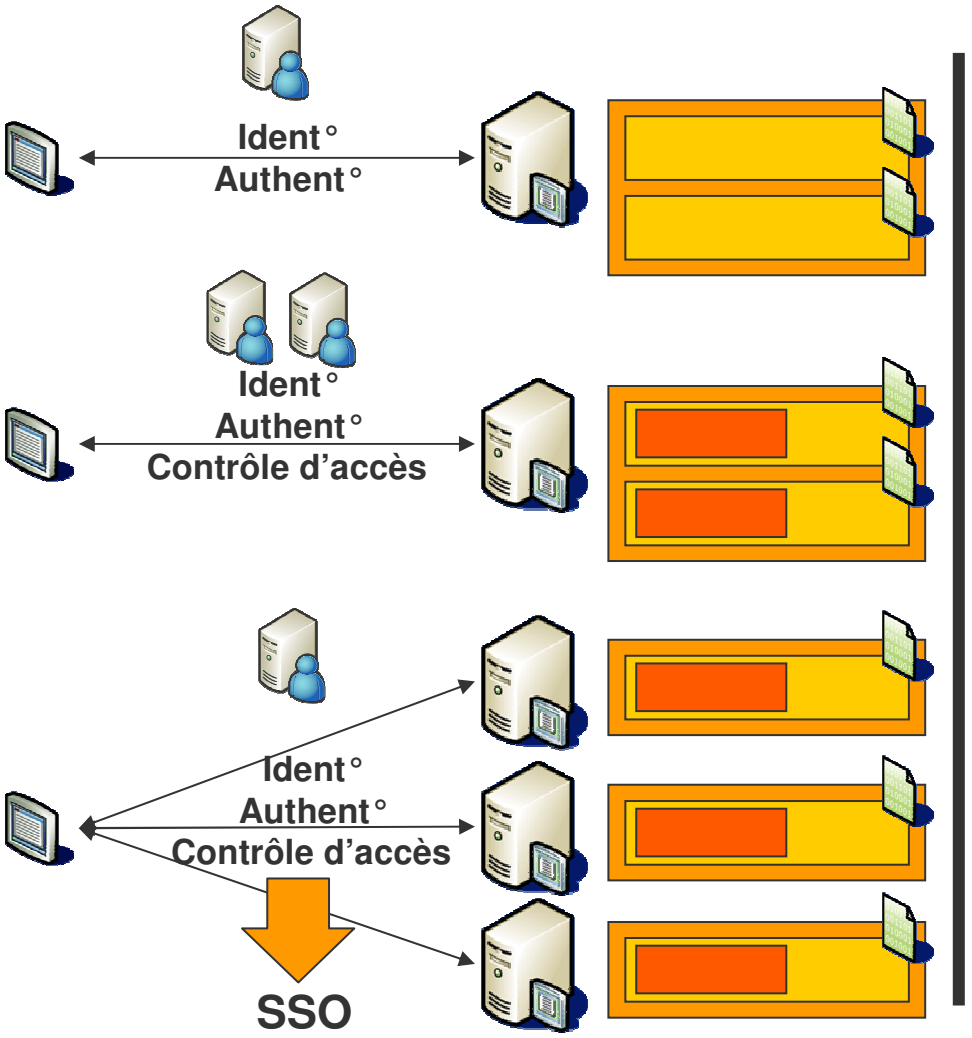
- rebond
  - point d'entrée privilégié
  - atteindre des machines internes
  - relais pour attaques externes

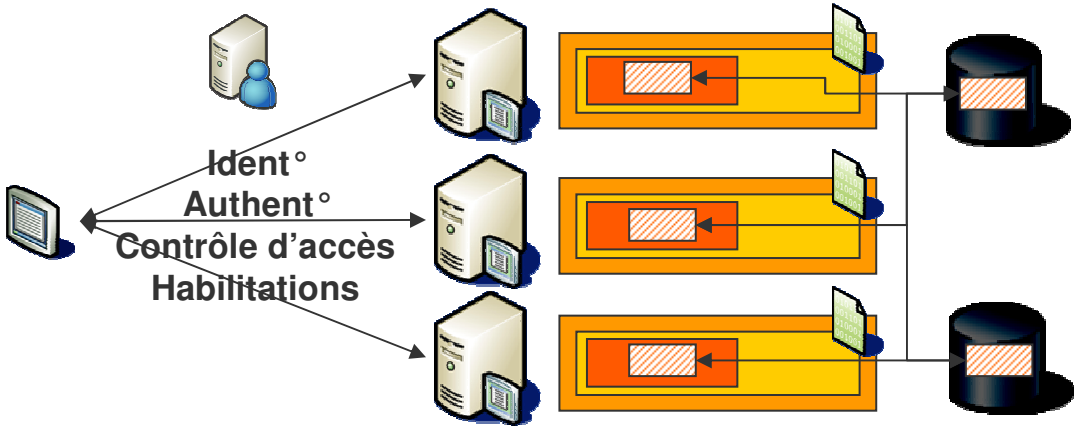
évolution des architectures applicatives

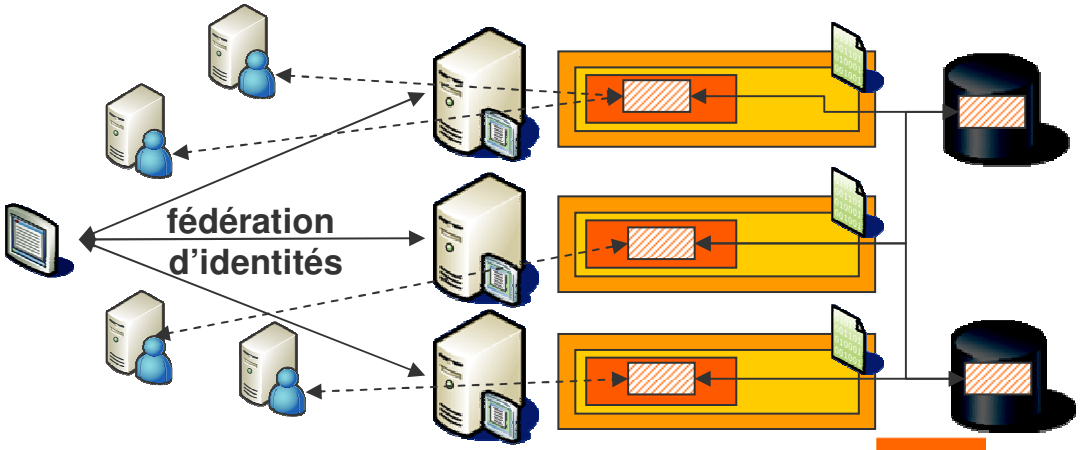
> des applications monolithiques vers des applications distribuées



approche globale de la sécurité applicative
de plus en plus d'exigences de sécurité…







Business Services orange

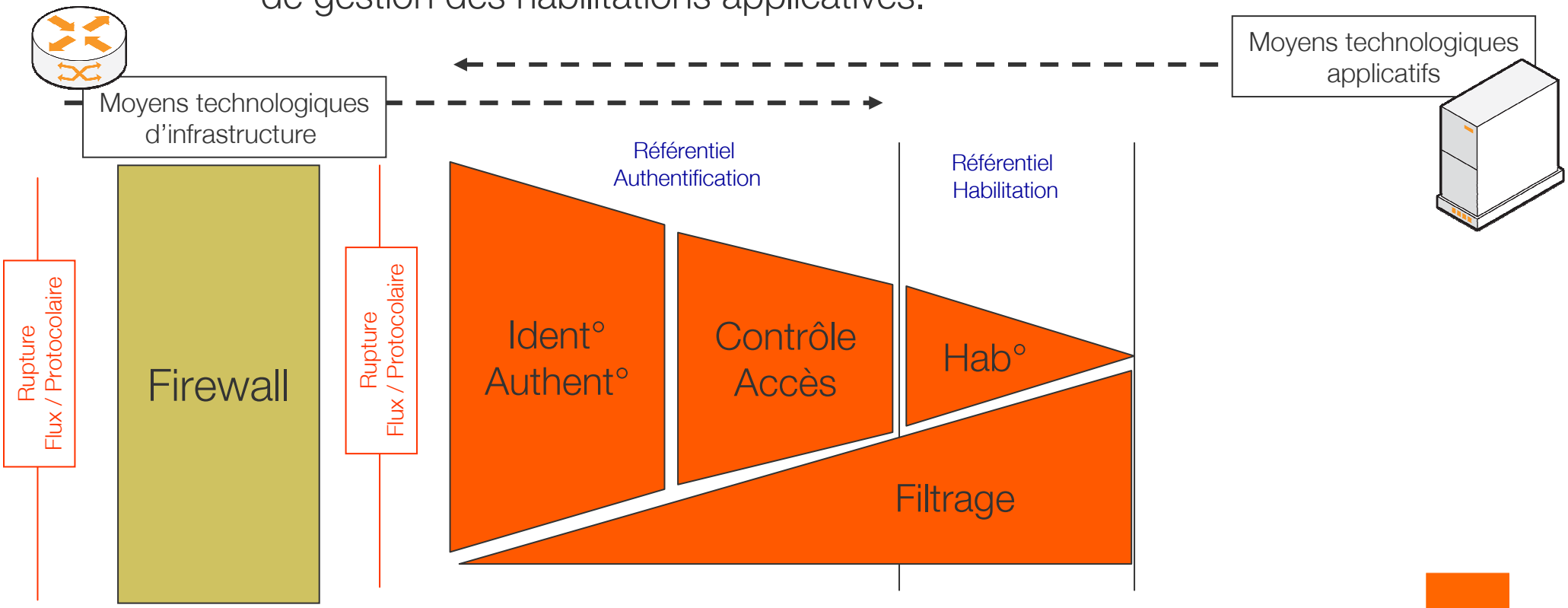
deux tendances fortes

> ne plus gérer les utilisateurs dans les applications
  - identité / profil / rôle
  - dépendance trop forte / réactivité et pérennité des données

> se préparer à ne plus gérer [totalement] des opérations de sécurité
  - identification + authentification
  - contrôle d'accès
  - filtrage et inspection de contenu

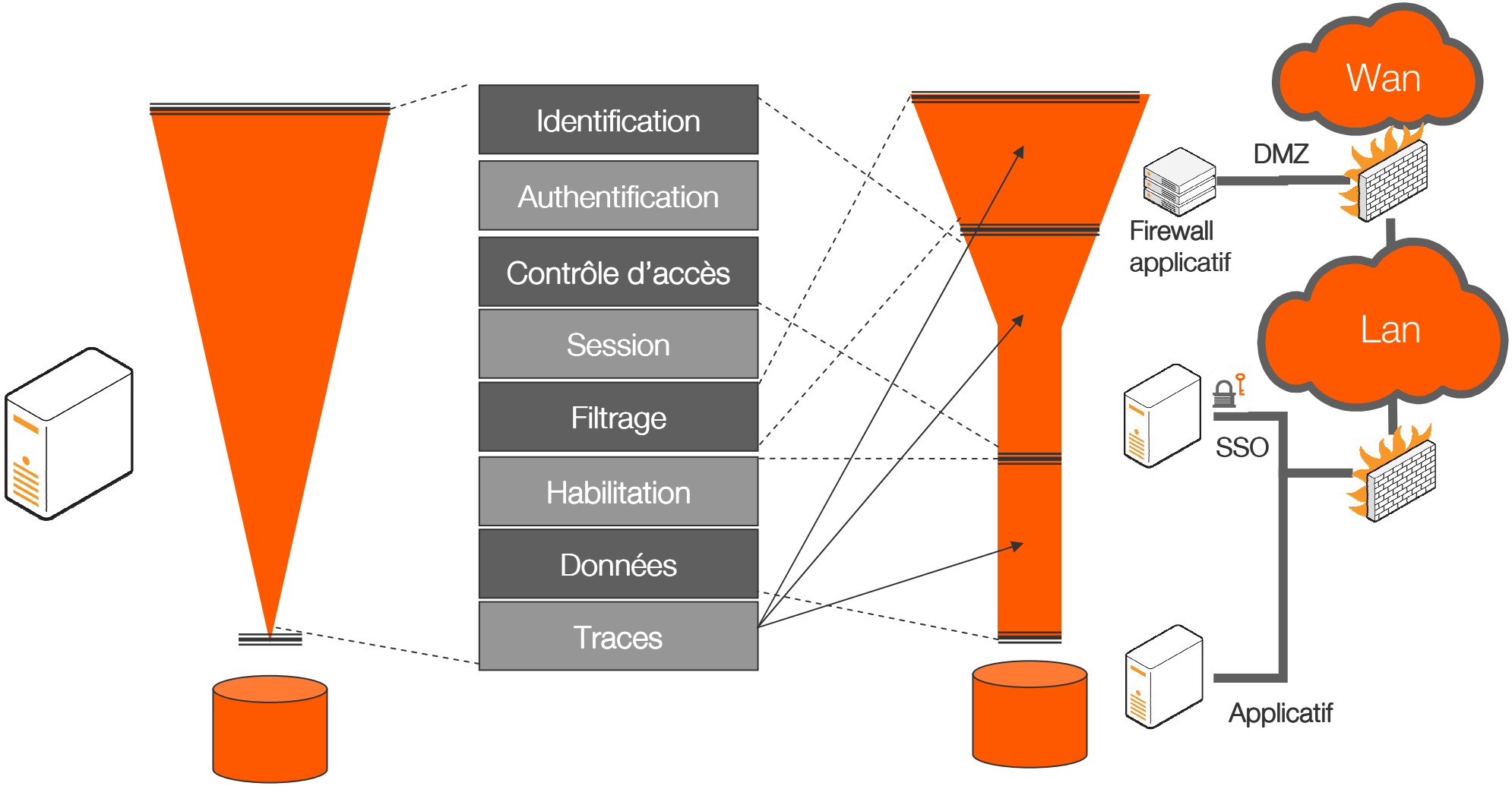
besoin en sécurité
complémentarité des solutions

> la solution peut passer par la complémentarité des moyens :
- d'authentification/identification,
- de contrôle d'accès,
- de gestion des habilitations applicatives.



Business Services orange

besoin en sécurité
des modèles d'architecture

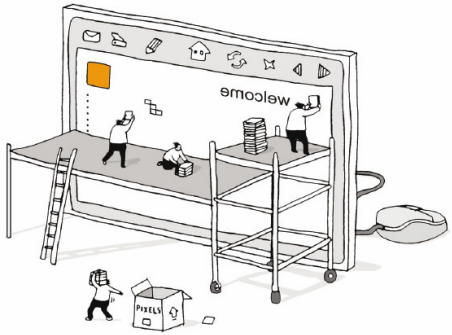


Business Services orange

les vulnérabilités des applicatifs Web

> 3 origines :

- poste Client :
  - code hostile (Virus, vers, etc.),
  - contrôles ActiveX, Applets Java
  - RIA et RDA
- canal de communication :
  - pas de mécanisme de sécurité dans IPv4
- serveurs :
  - "Front-End" : Serveurs HTTP/HTTPS frontaux
  - scripts CGI : écrits en perl, python, etc. et exécutés sur le serveur
  - "Middlewares" : Bus de communication ou Services Web permettant la distribution des composants logiciels
  - "Back-End" : Bases de données



typologies d'attaques applicatives Web

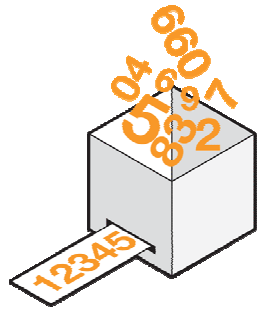
> plus de 70% des applications web présentent des vulnérabilités :

- responsabilité de l'application
  - XSS
  - Injection
  - CSRF
  - usurpation de paramètres
  - modification de cookies
  - …
- responsabilité du conteneur
  - serveur SGBD
  - serveur Web
  - …

les mécanismes de sécurité impliqués dans la protection des principales attaques

	Typologie d'attaques	Identification	Authentification	Contrôle d'accès	Filtrage et inspection de flux	Habilitations	Traces et journalisation	Utilisation de ressources cryptographiques
A1	Cross Site Scripting (XSS)				X			
A2	Paramètre non validé				X			
A3	Exécution de fichiers malicieux				X			
A4	Référence directe d'objets non sécurisé	X	X	X		X		
A5	Cross Site Request Forgery (CSRF)				X			
A6	Mauvaise gestion des erreurs						X	
A7	Violation de Gestion d'Authentification et de Session	X	X	X		X		
A8	Stockage non sécurisé							X
A9	Communication non sécurisée							X
A10	Violation de Contrôle d'Accès	X	X	X				

tendance



> les menaces sont passées du réseau à l'application
  - vulnérabilités applicatives sont graves, exploitables, exploitées

> les applications sont vulnérables, puisque …
  - chaque application est unique, exposant son propre lot de vulnérabilités
  - chaque application est développée avec une part de nouveauté technologique et donc de risque
  - chaque application devient multimodale avec des fonctionnalités complexes avec l'avènement du Web 2.0 et de la SOA

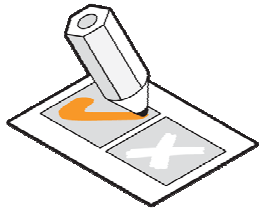
> contrairement à la sécurité de l'infrastructure où les pirates attaques des protocoles, au niveau applicatif la cible est l'application elle-même
  - l'impact sous-jacent est nécessairement au moins plus important !

processus de développement

> un processus à part entière du développement
  - applications en projet
    - prise en compte de la sécurité dès le début du projet
    - bonnes pratiques de développements
    - mécanismes de sécurité
    - tests adaptés
  - applications en production
    - audits de sécurité technique : revue de code, audits, tests d'intrusion
> outils automatiques
  - accélère la découverte
  - permet de se concentrer sur les points importants, pour l'outil retenu
  - faux positifs à confirmer
  - non exhaustifs : certains tests non couverts

  → nécessité d'un contrôle manuel complémentaires

perspective



- remonter la sécurité le plus en amont possible
  - passage d'architecture n tiers vers n+1 tiers, avec une couche, logique ou physique, dédiée à la sécurité
  - capitaliser sur l'implémentation des fonctions de sécurité portées par le serveur d'application ou par des frameworks dédiés
  - mise à disposition de « services de sécurité » pour les équipes de développement concentrées sur le développement de la logique métier
    - accélération des phases d'intégration et de déploiement
- gérer les exigences et spécifier la sécurité de l'application comme n'importe quelle fonctionnalité … critique
- élévation naturelle du niveau de sécurité de l'architecture
  - faire appliquer la politique de sécurité maîtrisée
  - d'un point de vue technique, cela repose sur une combinaison de moyens portés par l'infrastructure et l'applicatif
- faire évoluer nos mentalités
  - hier, je livrais du code
  - aujourd'hui, je livre du code de qualité
  - demain, je livrerai du code de qualité et sécurisé
    - il faut se préparer à apporter des éléments d'appréciation des moyens mis en oeuvre


merci