gemalto
security to be free

Authentication in the cloud – Breaking down the dilemma of compromising security Vs convenience

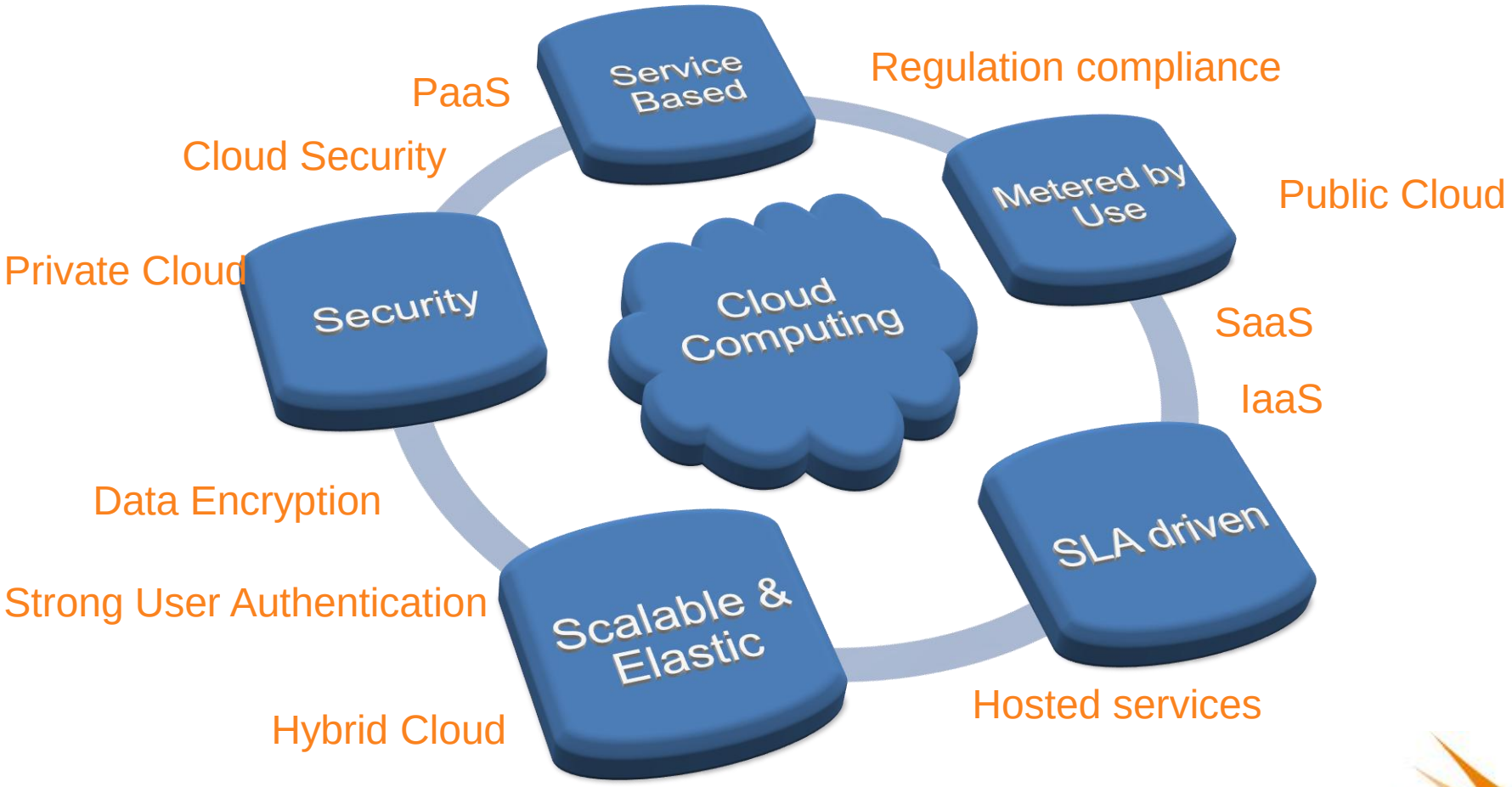
October 2010

If you are planning to move parts of your IT into the cloud, or have already done so, are you sure who is going to access it? You want to cede control to your data but not on who uses it, right? Authenticating who can manipulate your sensitive information in the cloud can come with its own challenges.

This presentation will try to breakdown the dilemma of compromising security Vs convenience by showing the attributes that are necessary of Strong 2FA and that having your cake and eating it too is actually possible if you keep your users behavior in mind when it comes to authentication in the cloud.

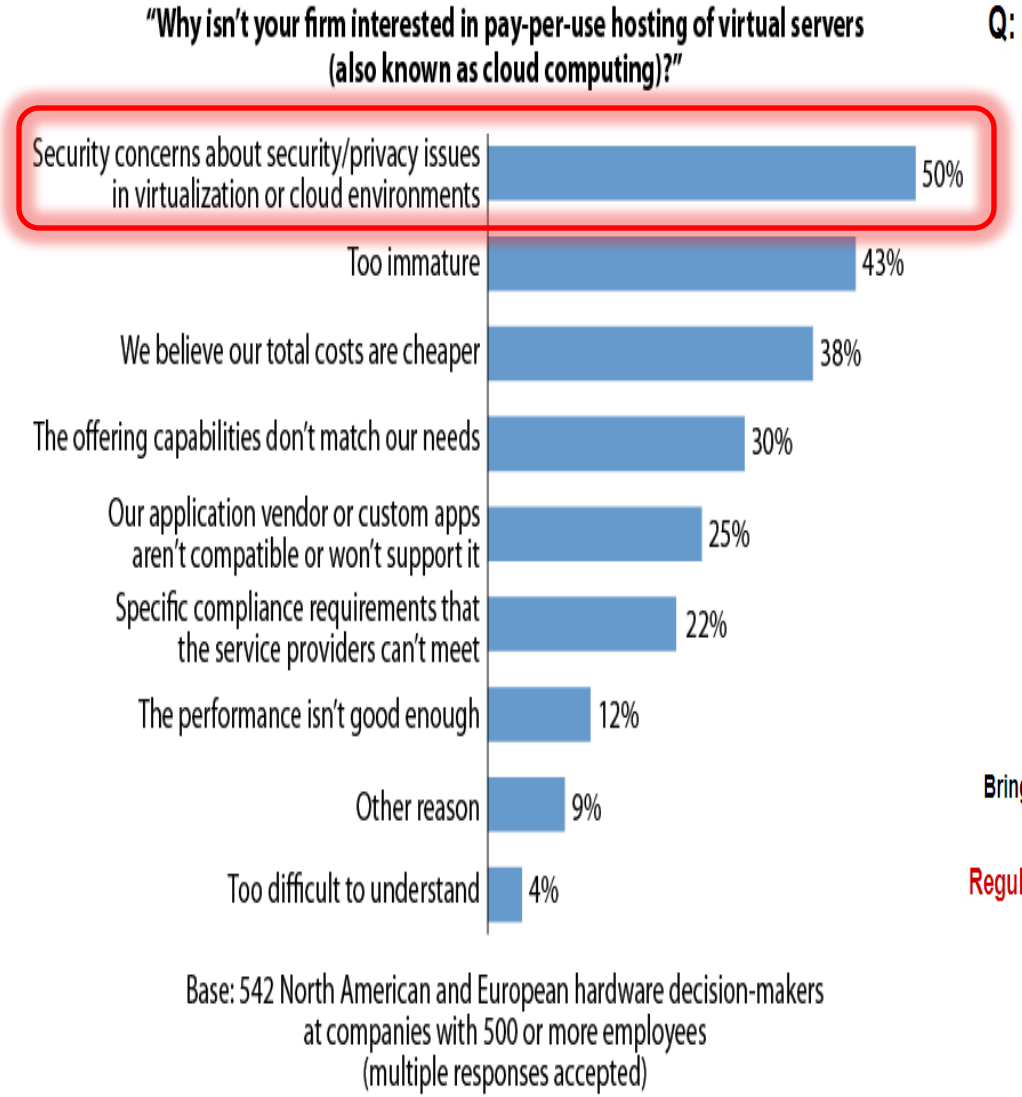
Attributes of Cloud Computing

NIST definition of Cloud Computing *Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*

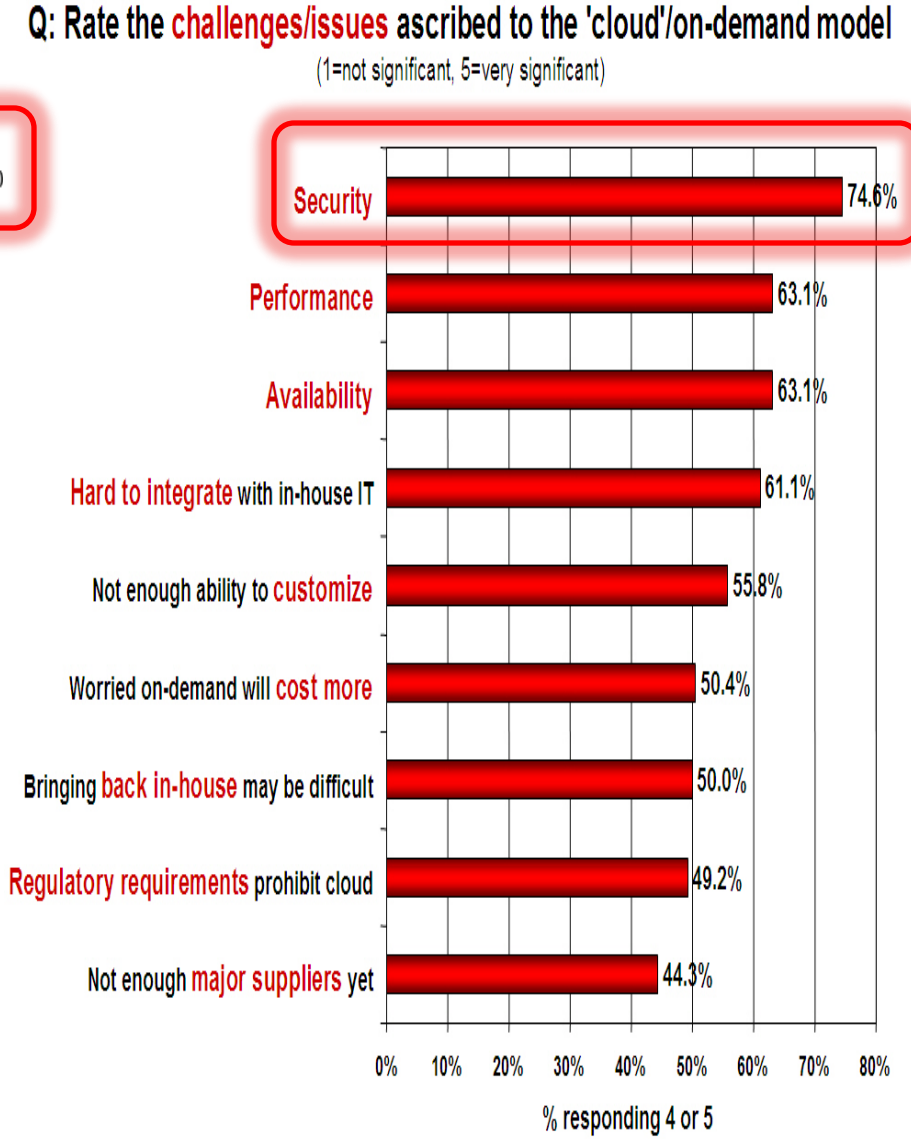


“Security” is important in the cloud

– though no real regulations yet

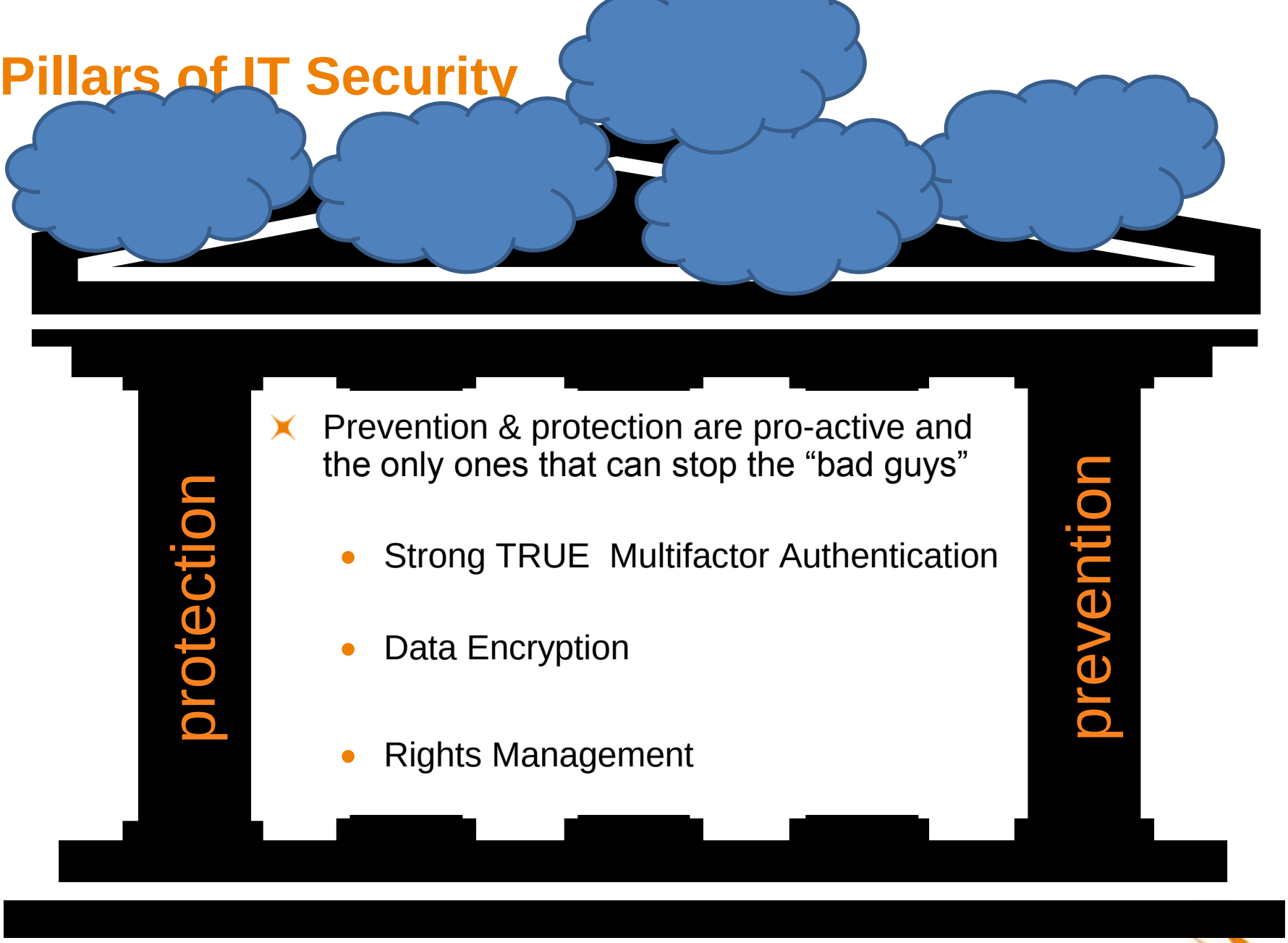


Source: Enterprise And SMB Hardware Survey, North America And Europe, Q3 2009



Source: IDC Enterprise Panel, August 2008 n=244

Pillars of IT Security



- Prevention & protection are pro-active and the only ones that can stop the “bad guys”
  - Strong TRUE Multifactor Authentication
  - Data Encryption
  - Rights Management

Challenge: Balancing Security, Convenience & Cost

- Security
  - Implementing the right level of security according to the anticipated risk level – not more, not less
- Convenience
  - Preserving the online convenience for end-users is essential, particularly in ***cloud computing***
- Cost
  - Overall cost, including recurring costs have to be optimized and fully controlled. In the ***cloud*** scenario, the “pay as you go” utility model is very critical

The best security measures are the ones people actually use !

Attributes of strong, usable 2FA authentication

- Non intrusive to allow anywhere access
  - “0 footprint” or embedded in operating system
  - Leverage Identity federation, allow identity aggregation
- Standard based to ensure vendor neutrality
  - OATH, X509, EMV CAP, SAML 2
- Portable so that user will always have their credentials
  - In the wallet, on your phone, becomes your flash drive
- Intuitive to use to avoid learning and change fear factor
  - 5mn learning curve
- Adapted to the risk profiles
  - To protect identities from phishing to man in the browser and identity sharing
- Deployment compatible with cloud principles
  - Web based & seamless user experience (like Amazon 1 click)
  - No pain for the service provider (no device handling, fulfillment & with auto provisioning)
  - “metered” pricing model
- Available everywhere your customers are

Authentication as a Service – Offer components

- Hosted Service (available in the cloud itself keeping with the need)
  - Fully managed hosted Authentication Server
  - Simple “snap-on” to existing infrastructure
- Good security story to support moving authentication to the cloud
- High availability assurance and Robust SLA
- User friendly web portals for Admins and Users alike (credential/token management)
- Order management
  - Web based with incremental user payment
  - Fulfillment service for delivery of authentication device direct to end users
- Open Standards
  - SAML 2.0
- Regulations and audits to consider
  - SAS 70

Ideal end-user interaction