

The Evolution Of Identity and Access Management for the Cloud

Tim Dunn
VP Security Strategy Europe

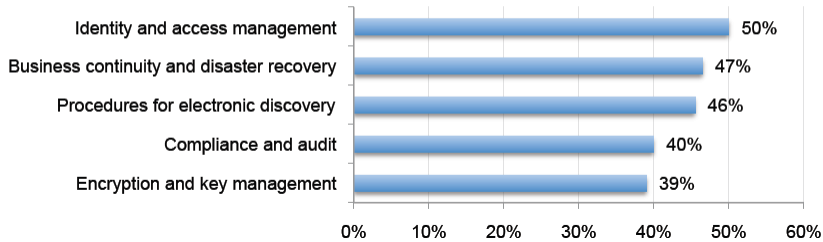


Cloud Adoption Concerns: 87.5% rate cloud security issues as "very significant" IDC Survey



#1 Area of Needed Focus for Migration to the Cloud? IAM!

Bar Chart 15
The top five critical areas of focus for organizations migrating to the cloud environment
Important & very important response for US and EMEA combined



Security of Cloud Computing Users – A Study of US & EMEA IT Practitioners, Ponemon Institute

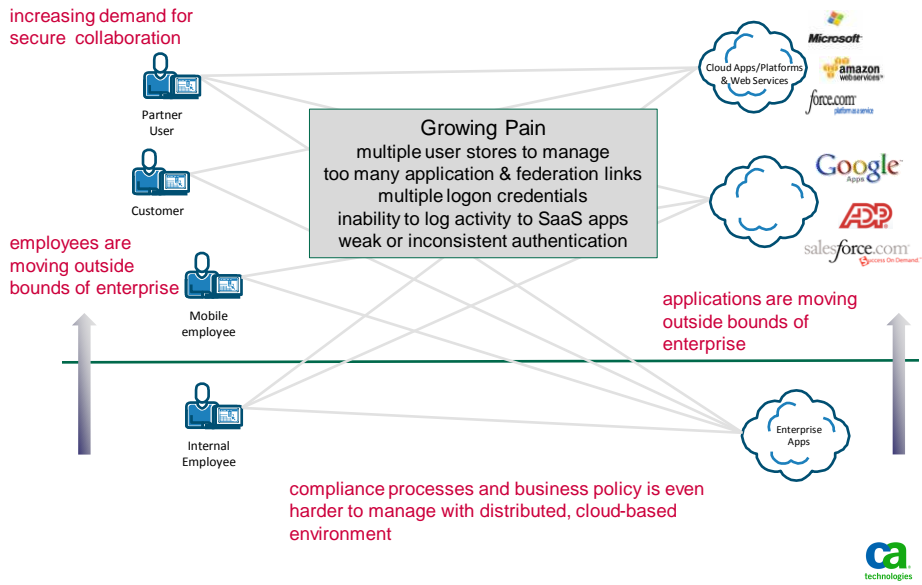


Why is Identity and Access Management Important?

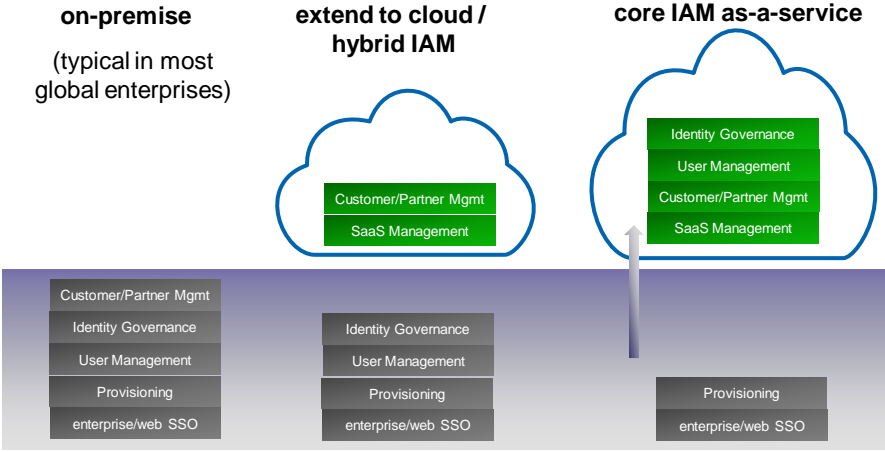
<p>SaaS Adoption</p>		<p>Nearly 90 percent of organizations surveyed expect to maintain or grow their usage of software as a service (SaaS), citing cost-effectiveness and ease/speed of deployment as primary reasons for adoption, according to a recent survey by Gartner</p>	
<p>Mobile Workforce</p>		<p>By the end of 2013 mobile worker population is expected to exceed 75% and to 1.19bn globally.</p>	
<p>Customer Confidence</p>		<p>Over 70% people surveyed believe authentication effects the degree of customer trust in the security offered.</p>	
<p>Increasing eCrime</p>		<p>More than 11 million adult consumers became victims of identity fraud in 2009, up from nearly 10 million in 2008. The number of fraud victims rose for the second year in a row</p>	
<p>Regulatory Pressures</p>		<p>Organizations that regularly review and maintain compliance with leading industry security standards and regulations spend about three times less annually than organizations that fall out of compliance.</p>	



distribution of users and applications is creating a complex environment



Evolution of IAM for the Cloud enabled Enterprise



CA's Security strategy



Content-Aware IAM

- Bring content to identity and identity to content



Secure virtualized environments

- Manage the complexity of securing virtualization
- Extend the controls into the hypervisor
- Visibility & control to enable IaaS adoption



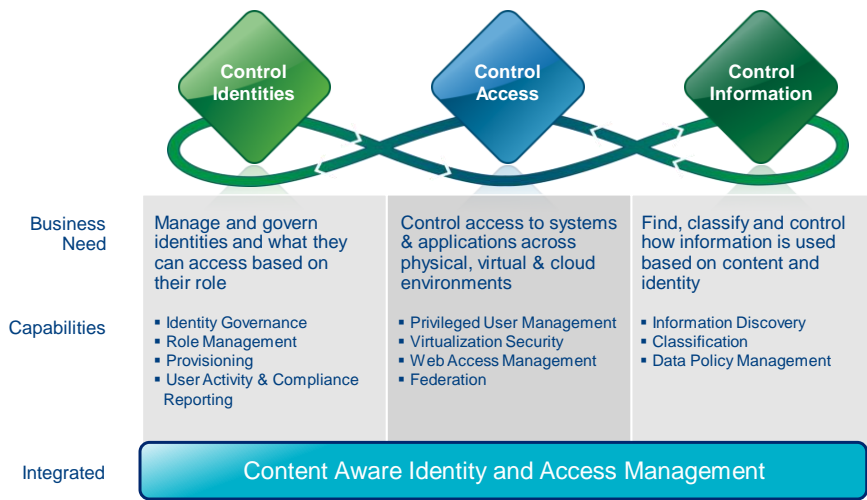
IAM & Cloud adoption

- Extend enterprise security to, for, from the Cloud
- Vertically focused communities of trust
- Partner with service providers (HiTRUST, Acxiom, Mycroft, WiPro, BT,...)



Security Building Blocks of Success

The control you need to confidently drive business forward



CA's Security strategy



Content-Aware IAM

- Bring content to identity and identity to content



Secure virtualized environments

- Manage the complexity of securing virtualization
- Extend the controls into the hypervisor
- Visibility & control to enable IaaS adoption



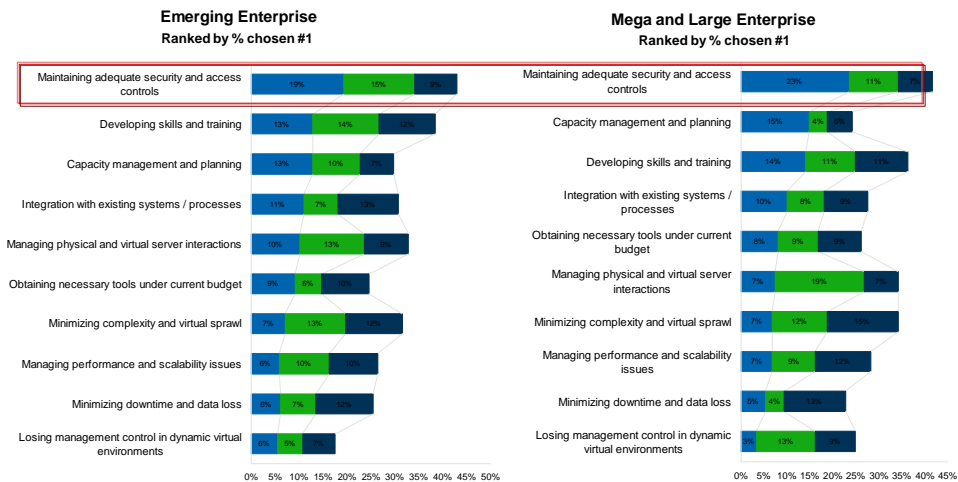
IAM & Cloud adoption

- Extend enterprise security to, for, from the Cloud
- Vertically focused communities of trust
- Partner with service providers (HITRUST, Acxiom, Mycroft, WiPro, BT,...)



Maintaining Adequate Security and access controls is the #1 Customer Challenge

What are the greatest challenges you face in virtual server management?

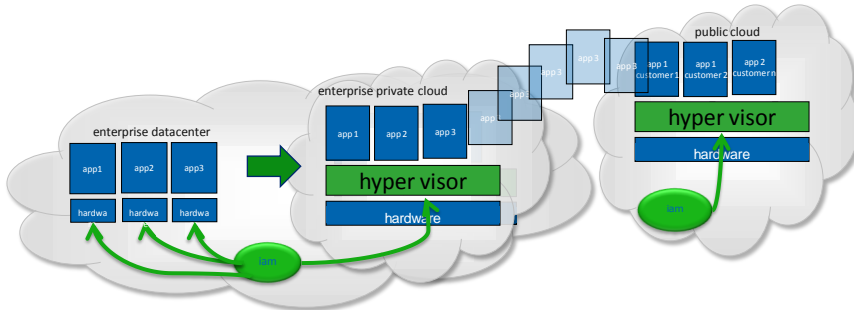


Source: Emerging Enterprise: N = 325, Mega / Large: N = 148



How do I secure virtualized environments? Two Primary Issues:

1. Managing access by Privileged Users' on the Data Centre Infrastructure
2. Extending and automating IAM controls in Virtualised / Cloud Applications



CA's Security strategy



Content-Aware IAM

- Bring content to identity and identity to content



Secure virtualized environments

- Manage the complexity of securing virtualization
- Extend the controls into the hypervisor
- Visibility & control to enable IaaS adoption



IAM & Cloud adoption

- Extend enterprise security to, for, from the Cloud
- Vertically focused communities of trust
- Partner with service providers (HiTRUST, Acxiom, Mycroft, WiPro, BT,...)



cloud security

Cloud Security

To

Extend enterprise security to include security to cloud based applications including SFDC, Google, etc

For

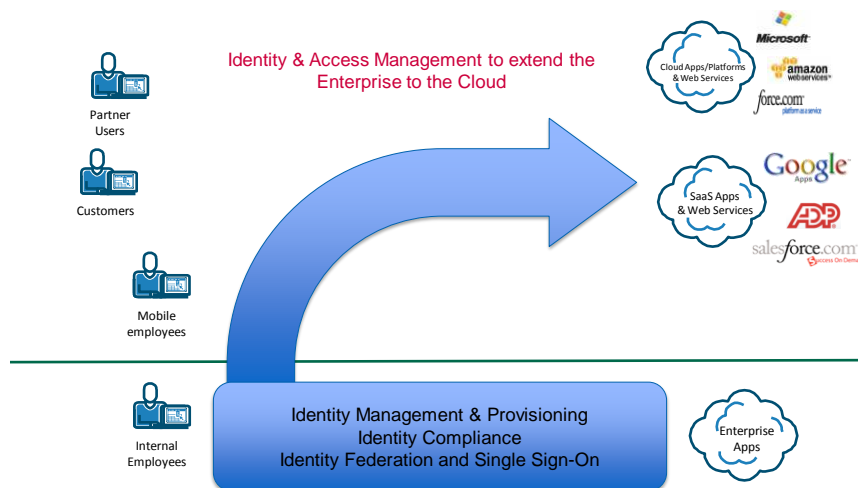
Security for cloud providers to ensure they meet the same level of security as within the enterprise

From

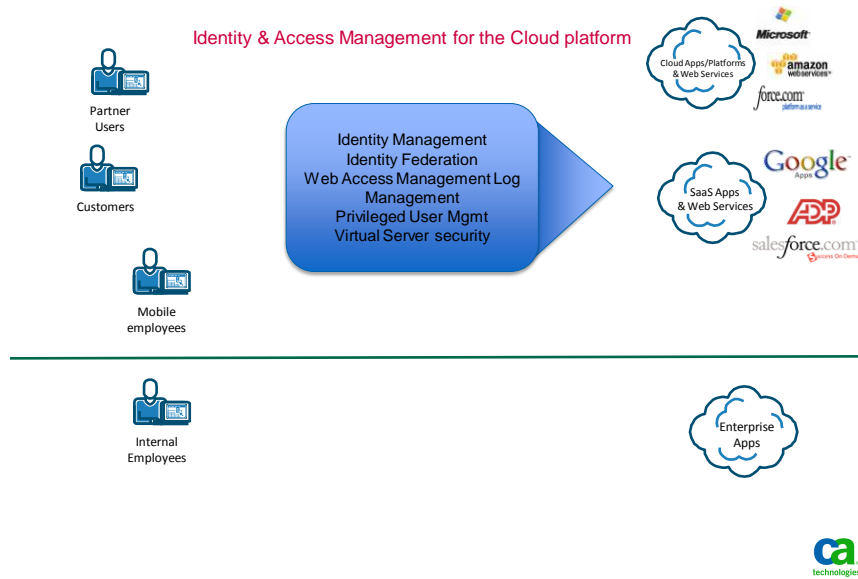
Security as a Service from the cloud including Authentication, Identity Management, Federation and SSO



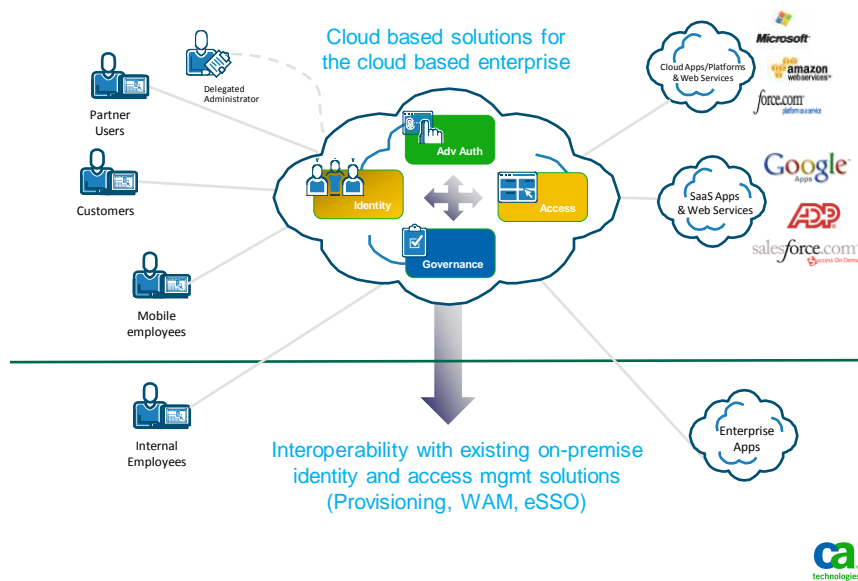
“To the cloud”: Extend on-premise IAM to Cloud applications



“For the cloud”: Enable service providers to deliver secure solutions with On-Premise IAM



“from the cloud”: cloud based solution is critical to gaining collaboration and SaaS efficiencies



Identity Assurance

Problem:

- Password is just not good enough anymore
- Hard tokens are expensive & difficult to use
- Multi-factor should only be used if needed

Solution:

- Multi-factor authentication transparent to the end user (certificate on device)
- One time passwords using mobile phone
- Adaptive authentication based on risk of user or the transaction
- Identity verification via personal questions

Business Benefits:

- Dramatically reduced capital & operational costs for multi-factor
- Business agility
- Better experience for customers and employees

Increase assurance with enhanced user authentication

Identity Assurance

Securely connect customers and partners to enterprise applications

Cloud Access Management

Ensure linkage between identity and applications follows business policy

Identity Governance



Cloud Access Management External user scenarios

Coming Soon

Problem:

- Lots of consumer identities to manage
- Many partner relationships to manage
- Multiple apps need to be shared with cust
- Apps are moving to Cloud (SaaS based)
- This is not core function of their business

Solution 1: Consumer Access

- Cloud based directory
- Self-service password & profile mgmt
- Single sign-on to multiple applications

Solution 2: Bus Customer & Partner Access

- Delegated administration for partner's users
- Federation with business customers & partners
- Single sign-on to multiple applications

Business Benefits:

- Dramatically reduced costs
- Business agility
- Better experience for their customers

Increase assurance with enhanced user authentication

Identity Assurance

Securely connect customers and partners to enterprise applications

Cloud Access Management

Ensure linkage between identity and applications follows business policy

Identity Governance



Cloud Access Management Internal employee scenarios

Coming Soon

Problem:

- Many new SaaS applications
- Loss of identity control & password policy
- No auditing of actual usage
- Multiple authentication actions for users

Solution 1: Cloud based employee mgmt

- Cloud based user directory
- Full access request & approval workflows
- Provision & de-provision users to SaaS
- Single sign-on to SaaS apps

Solution 2: Enterprise bridge to cloud

- Synchronize on-premise to cloud policy
- Provision & de-provision users to SaaS
- Authenticate against on-premise dir
- Single sign-on to SaaS apps & VPN
- Auditing and reporting of all user access

Business Benefits:

- Dramatically reduced helpdesk costs
- Business agility thru efficient use of SaaS
- Better experience for users
- Secure, compliant use of SaaS

Increase assurance with enhanced user authentication

Identity Assurance

Securely connect employees to cloud & partner applications

Cloud Access Management

Ensure linkage between identity and application follows business policy

Identity Governance



Identity Governance

Coming Soon

Problem:

- Ensuring business & compliance policy (SOD) is properly configured is very difficult
- Access certification is required but often a very manual and expensive process
- Collecting audit logs & verifying policy compliance is complex and manual

Solution:

- Definition & analysis of business/compliance policy (SOD)
- Clean-up of entitlements
- Access certification & attestation
- Identity risk dashboard
- Reporting of actual usage with policy

Business Benefits:

- Dramatically reduced compliance costs
- Better experience for business managers performing access certification

Increase assurance with enhanced user authentication

Identity Assurance

Securely connect customers and partners to enterprise applications
Securely connect employees to cloud & partner applications

Identity Federation

Deliver identity intelligence to enable the business to make better decisions

Identity Governance



Identity & Access Management Cloud Services

Enable secure, simplified access for business collaboration

Identity Assurance

- Provide transparent multi-factor authentication or mobile phone based one-time passwords across SaaS and enterprise apps
- Risk-adaptive authentication based on user and/or transaction
- Credential issuance and lifecycle management

Cloud Access Management

- Register and manage customer & partner identities directly to an on-demand service with self service & delegated administration
- Enable single sign-on to enterprise and SaaS apps
- Synchronize with on-premise identity or enable full identity lifecycle management from cloud based service

Identity Governance

- Access certification, business policy (SOD), identity risk rating
- Audit all access to SaaS and cloud applications



Thank you

