Follow the Money

How Cloud Providers' Business Needs Drive Enterprise Identity & Security

Kuppinger Cole + Partner European Identity Conference 2010

Dale Olds, Distinguished Engineer, Cloud Security Services

dolds@novell.com

https://virtualsoul.org

Novell

Agenda

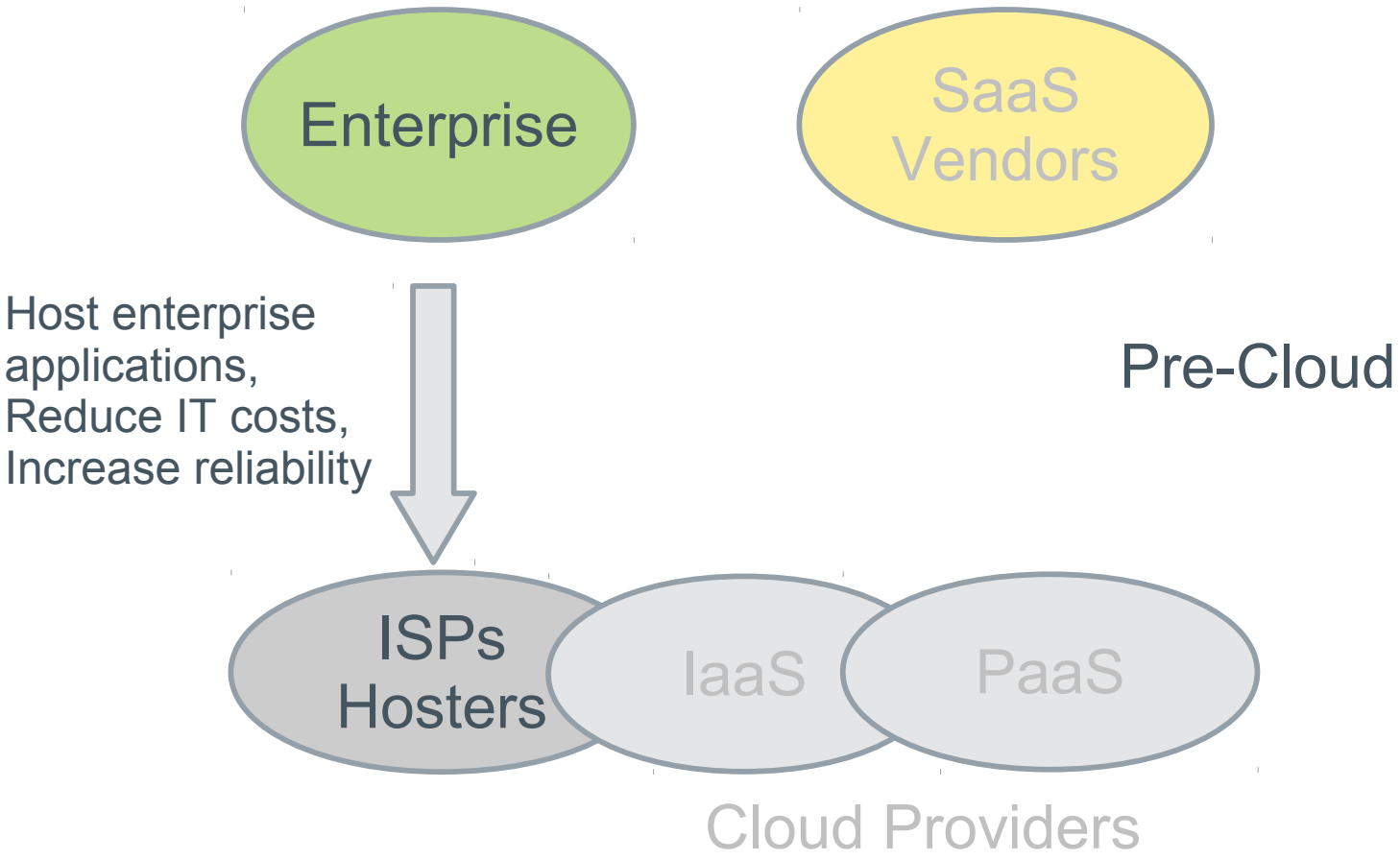
- Identify business drivers behind the shifting landscape of enterprise IT, SaaS vendors, and cloud providers
- Anticipate resulting trends and their implications for security and identity systems
- Put it all together with some recommendations


The Shifting Landscape of Enterprise IT, SaaS Vendors, and Cloud Providers

A Series of Shifts in the IT Landscape

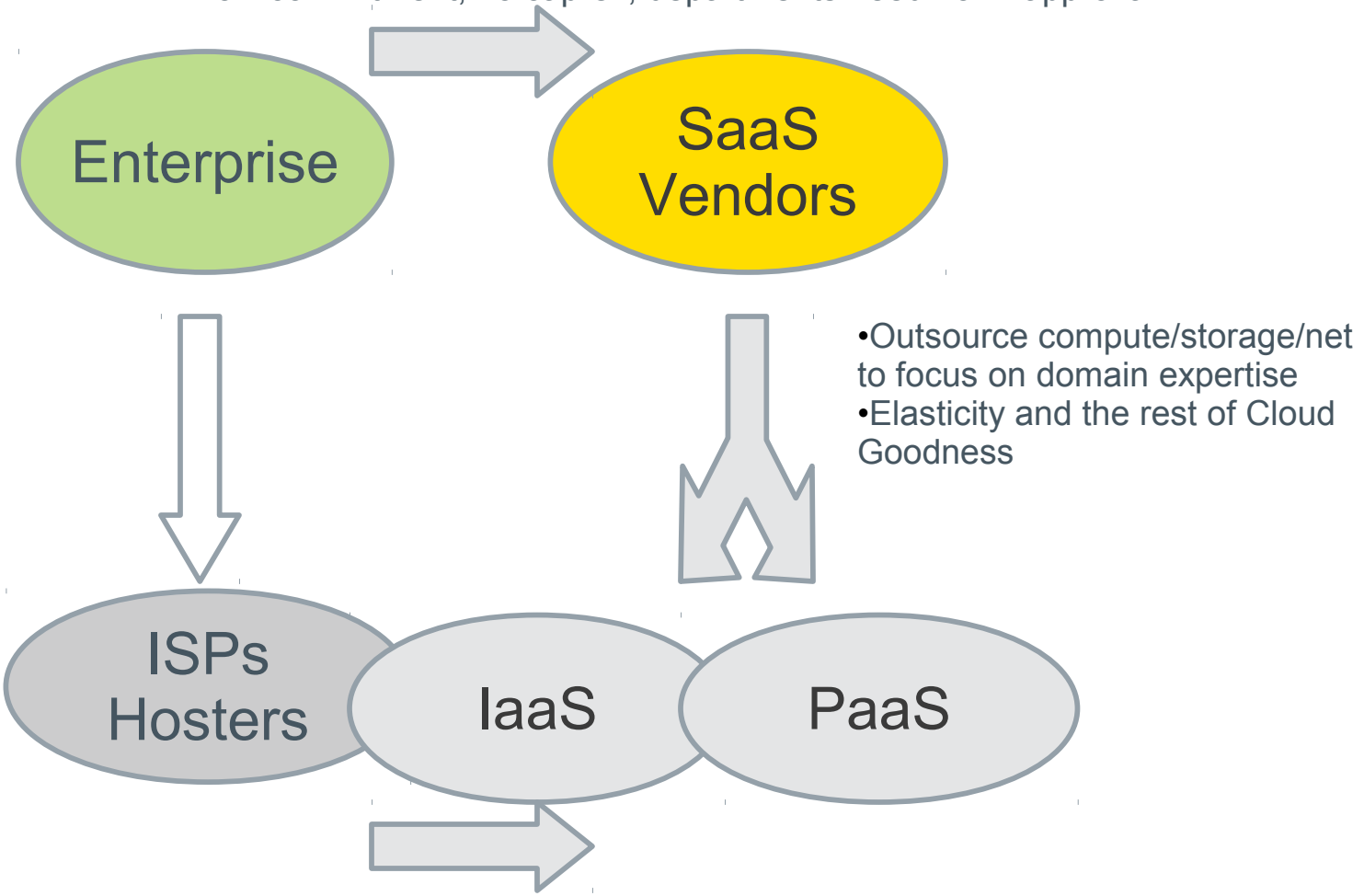
- Mainframe to mini computing
  - For example, the Digital Equipment Corporation Programmed Data Processors such as the PDP-11
- Mini and mainframes to PCs and Macs
- Workgroup networks and NetWare
- Open Source: Linux, Apache, etc.
- Cloud computing and SaaS
- In all of these cases, the **driving force** was **departmental autonomy pulling in products and services under the enterprise IT radar**

The Players: Enterprises, SaaS Vendors, Hosters/Cloud Providers



Motivations for the Shift to the Cloud

•Easy to try, and use deep domain expertise
•Low commitment, no cap-ex, departments need no IT approval



What Enterprises, SaaS vendors, and Cloud Providers Want Now

- Enterprises want:
  - Easy and **simple to try, use, and discard**
  - **Deep domain expertise**, more easily accessed
  - No commitments, no cap-ex, no IT dept approval, etc.
- SaaS Vendors want:
  - Security and **reduced risks** for their customers – reduced liability
  - Focus on core competencies and domain expertise
  - **Increase and retain customers by building community** around their application
- Cloud Providers want:
  - Customer retention – **stickiness**
  - Value added services up the stack – **incremental revenue**
  - Lower administration and management costs – **automation**


Current Trends and Traps

Three Trends Affecting Cloud Evolution & Enterprise Security

1. **Identity-based security** is increasing in importance
   - Cloud services are pushing enterprises to emphasize identity-based security rather than network security
2. SaaS and IaaS are **converging on PaaS**
   - Infrastructure providers are moving up stack and applications need to be extensible... converging on platform services, including identity services.
3. **Cloud providers** are increasingly offering identity services – and **becoming identity providers**
   - Identity services provide much needed security, and stickiness.
   - Application marketplaces are growing around identity hubs


Trend 1:
Identity-based
Security is
Increasingly
Required

Identity-based Security

Cloud services are pushing enterprises to emphasize **identity-based security rather than network security** – information security rather than network security.

Network security services like SSL connections, firewalls, edge security devices **are insufficient** when accessing Cloud services.

"It could be that moving even more stuff to the cloud is what will cause the debates, design and actions to build in identity, claim, tokens, policies and related security services. ***You can't hide behind a facade of 'network security' when there is no network.****"*

From Gunnar Peterson, 1raindrop.typepad.com

Separating identity sources from applications that securely use identity information is essential – the **identity provider model**

Authentication Methods Supported by SaaS Applications

8 Authentication Methods supported: What authentication methods does your SaaS application support, if any? (Check all that apply)

(Respondents were allowed to choose **multiple** responses)

Response	20% 40% 60% 80% 100%	Frequency	Count
SAML1.1		8.7%	6
SAML2		20.3%	14
WS-Fed		4.3%	3
OpenID		8.7%	6
Information Cards		0.0%	0
Other, please specify:		24.6%	17
None		10.1%	7
Don't know		**36.2%**	**25**
		Valid Responses	**69**

- SAML2 was the most common authentication method supported of the methods tested with ¼ of SaaS Providers supporting, but another ¼ indicated supporting other authentication methods not listed.
- 1/3 of respondents were not aware of the specific authentication methods supported by their SaaS application.

Security Capabilities Customers Are Asking SaaS Providers About

9 SaaS Provider Cust Security Cap Req: Which of the following security capabilities are your customers asking about relative to your SaaS solution? (Check all that apply)

(Respondents were allowed to choose **multiple** responses)

Response	20% 40% 60% 80% 100%	Frequency	Count
Single sign-on		54.2%	45
Audit tracking in SaaS		**55.4%**	**46**
Provisioning of users to SaaS application		48.2%	40
Support for multiple security standards (SAML, WS-FED, etc.)		18.1%	15
Multi-factor authentication		26.5%	22
Hosted or outsourced identity and access management		26.5%	22
None of the above		12.0%	10
		Valid Responses	83

- Audit tracking, Single sign-on and Provisioning of users were the three main security capabilities customers are asking SaaS providers about; about ½ of SaaS providers indicated customers asked them about these capabilities.

Trap: Don't Be Lulled by Exclusive Focus on Authentication and SSO

- **Externalized authentication** and the identity provider model is essential, urgent, and solvable now – it's the **lowest hanging fruit**
- BUT externalized authentication is just the first step and is **not sufficient** for security in the cloud
  - There are huge benefits of less identification – more externalized authorization.
    - See “Identity Crisis” by Jim Harper
  - Claims, policies
  - Transparency, audit, compliance
- **Externalized authentication is the means to an end**

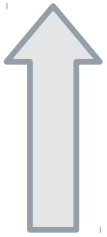
Trend 2: SaaS and IaaS are Converging on PaaS

SaaS and IaaS => PaaS

Extensibility, Customizability, Community

Common services e.g. billing, identity, load balancing, elasticity of storage and compute, etc.

Value added services, billing, SLAs



Software as a Service

Pivotlink, Salesforce, Netsuite, Taleo, SuccessFactors. etc. Apps are secured by vendors

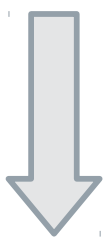
Platform as a Service

Google App Engine, force.com, Azure.

Infrastructure as a Service

GoGrid, Amazon EC2, Opsource, etc. Machine images are secured by vendors

Security Responsibilities



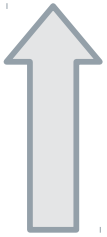
Software as a Service

Full application stack and infrastructure is secured by vendors – customer handles data in and out

?

Platform as a Service

Who is responsible for securing the application here?



Infrastructure as a Service

Machine images are secured by vendors, everything else is up to customer – no guarantees about running code, etc.

Trap: Don't Assume PaaS Security is like SaaS or IaaS

- Security responsibilities on PaaS applications are not so clearly delineated
- IaaS security responsibilities end at the virtual machine boundary – customer is responsible for security of all code above the hypervisor
  - http://www.voiptechchat.com/voip/457/amazon-ec2-sip-brute-force-attacks-on-rise/
- SaaS security responsibility is entire application code stack
- PaaS contains some customer code and some cloud provider code
- Know your security responsibilities

Trend 3:
Cloud Providers Are Adding Identity Services

Cloud Providers as Identity Providers

- Cloud providers are increasingly offering federated identity services – and becoming identity providers
- Identity providers in the sense of a federation hub and optionally user accounts
- Identity services provide much needed security, and stickiness.

*If ... Cloud operators want to woo mature enterprise customers to use their services, they are **leaving money on the table** and not fulfilling customer needs by failing to roll out complimentary security capabilities which lessen the **compliance and security** burdens of their prospective customers.*

From Chris Hoff, www.rationalsurvivability.com/blog

Primary Type of Hosting Environment SaaS Applications Use

5 Type Hosting Enviro: What primary type of hosting environment does your SaaS application use? (Choose one)

(Respondents could only choose a **single** response)

Response	20% 40% 60% 80% 100%	Frequency	Count
Our own servers		34.8%	24
Dedicated hosting through third party		**37.7%**	**26**
Cloud hosting through IaaS provider		27.5%	19
	Mean		1.928
	Standard Deviation		0.792
	Valid Responses		**69**

- Third Party dedicated hosting was the most common hosting environment used by 38%, but followed closely by the use of own internal servers by 35%. 28% indicated using Cloud hosting through an IaaS provider.
- All three show significant levels of usage by SaaS Providers.

SaaS Provider Preferred Method to Offer Security Capabilities to Customers

10 Saas Provider Security Cap Source Prefer: How would your organization prefer to offer the security capabilities you selected above to customers? (Choose one)

(Respondents could only choose a **single** response)

Response	20% 40% 60% 80% 100%	Frequency	Count
Refer them to a third-party vendor		6.0%	5
Build the functionality in-house		**34.9%**	**29**
OEM the solution from a third-party vendor		27.7%	23
Get as part of development platform		2.4%	2
Get as part of hosting environment		22.9%	19
No security capabilities requested/required		6.0%	5
	Mean		3.193
	Standard Deviation		1.435
	Valid Responses		**83**

- 1/3 of SaaS Providers prefer to build the requested security capabilities in-house … but 1/3 above were also unaware of their authentication methods.
- ¼ indicated they would prefer to OEM from a third party vendor and another ¼ indicated they would prefer to source as part of their hosting environment.

Cloud Providers and the Opportunity of a SaaS Marketplace

- Beyond providing common identity services to their SaaS customers, Cloud Providers benefit directly
  - Needed stickiness
  - Incremental revenue
- Explosive growth is possible with network effects of multiple SaaS vendors
  - User account (or federation broker) is the hub
  - Possible integration of other services
- Ultimately SLAs come from the cloud provider
  - Including identity as an integration service on that foundation is key to producing a platform

Examples

- Google Apps Marketplace
  - Common accounts via Google Apps
  - Federated to applications with OpenID
- Force.com
  - Common accounts via Salesforce.com
  - Federated with SAML
- Opsource
  - Billing for SaaS vendors
  - And as of last week, stronger SLAs
    - http://www.opsource.net/press/opsource-sets-new-sla-standard-cloud-computing-guarantees-cloud-reliability-perf
- Possible marketplace providers: Telcos, hosters

Traps: Cloud Provider Services vs SaaS & IDaaS Point Solutions

- Identity as a Service vendors
  - Exist between the enterprise and the SaaS vendor
    - Passport model – see Kim's Law of Justifiable Parties
  - Here now and not going away but may conflict with cloud providers growing tendency to be the identity provider
- Departmental adoption vs. identity provider operating on behalf of the enterprise
  - Market forces lead to cloud providers with common identity services hubs
  - But there are disjoint management boundaries between departmental adoption of SaaS and enterprise identity providers


Putting it all Together
with Recommendations

Summary

- Identity provider model is essential for cloud computing
- Increasing need for identity-based security in addition to network security
- SaaS and IaaS are moving toward PaaS, with undefined security responsibilities
- Identity services offered by cloud providers make sense
- SaaS marketplaces provide advantages to SaaS vendors, cloud providers – and enterprises

Recommendations

- There are many excellent **standards that support the identity provider model** – SAML, WS-Fed, OpenID, information cards – and shipping products that implement them. **Use them**.
- **Make your security needs known** to your SaaS vendors, hosters, cloud providers
- Look for **the rise of SaaS application stores** built around a **cloud provider hub** with common identity and security infrastructure. They are a good idea.
- Beware of the interplay between departmental use of Cloud services and IT control of the Identity Provider.
  - If you're an enterprise, it's politics.
  - If you're a cloud provider or identity services vendor, we still have technology design and standards work to do.


Thank you


Novell®