

# Cloud Security: Moving Beyond Single Sign-on in 2010

**Anita Moorthy**  
**Senior Solutions Manager**

**Novell.**

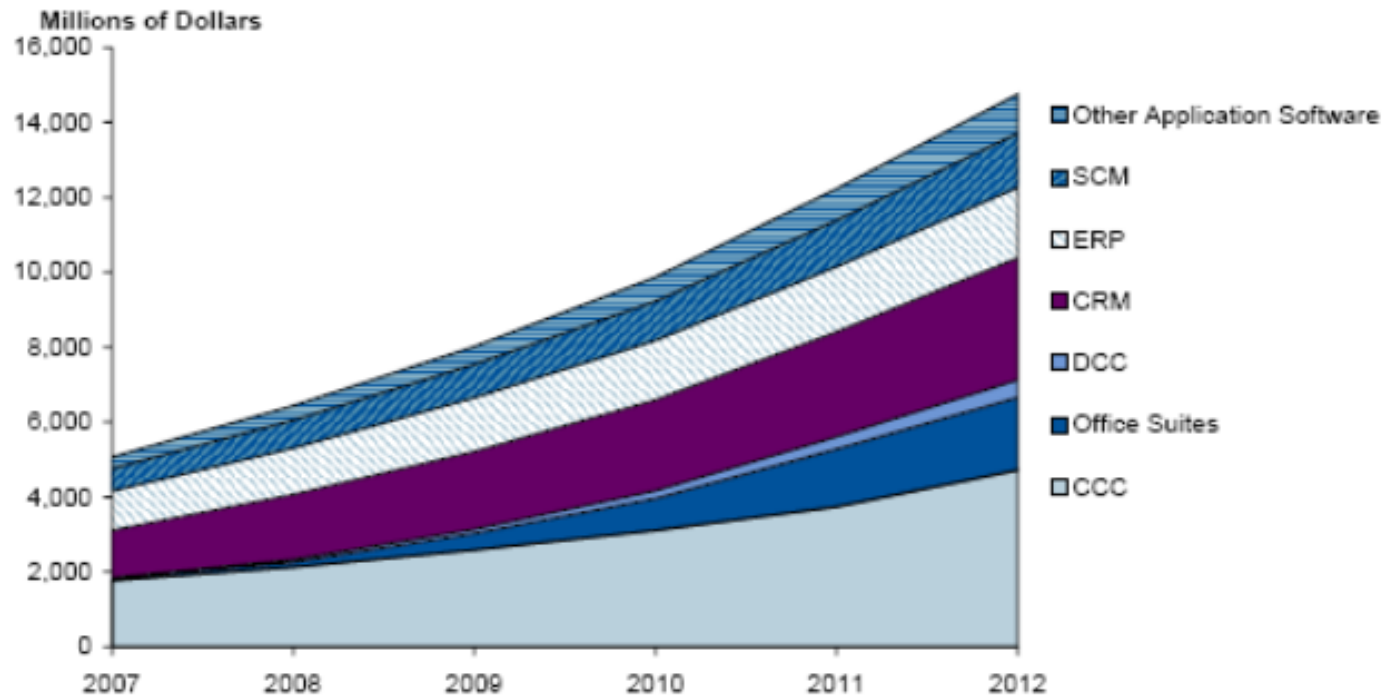
# Takeaways for Today

- SaaS adoption is projected to increase **three-fold** to \$14 Billion by 2012 according to Gartner
- Reality is that SaaS **adoption is still departmental** and piecemeal – it is not mainstream in most enterprises
- To **increase user adoption** of SaaS within an enterprise, you need to fit nicely within the IT policy and framework of an organization
- **Security** is a primary concern, but it comes in many guises
- Security is the **responsibility** of BOTH you AND your vendors of choice

What are your customers security concerns?

# SaaS Adoption Growing As Model Matures: \$8B in '09 to \$14.7B in '12

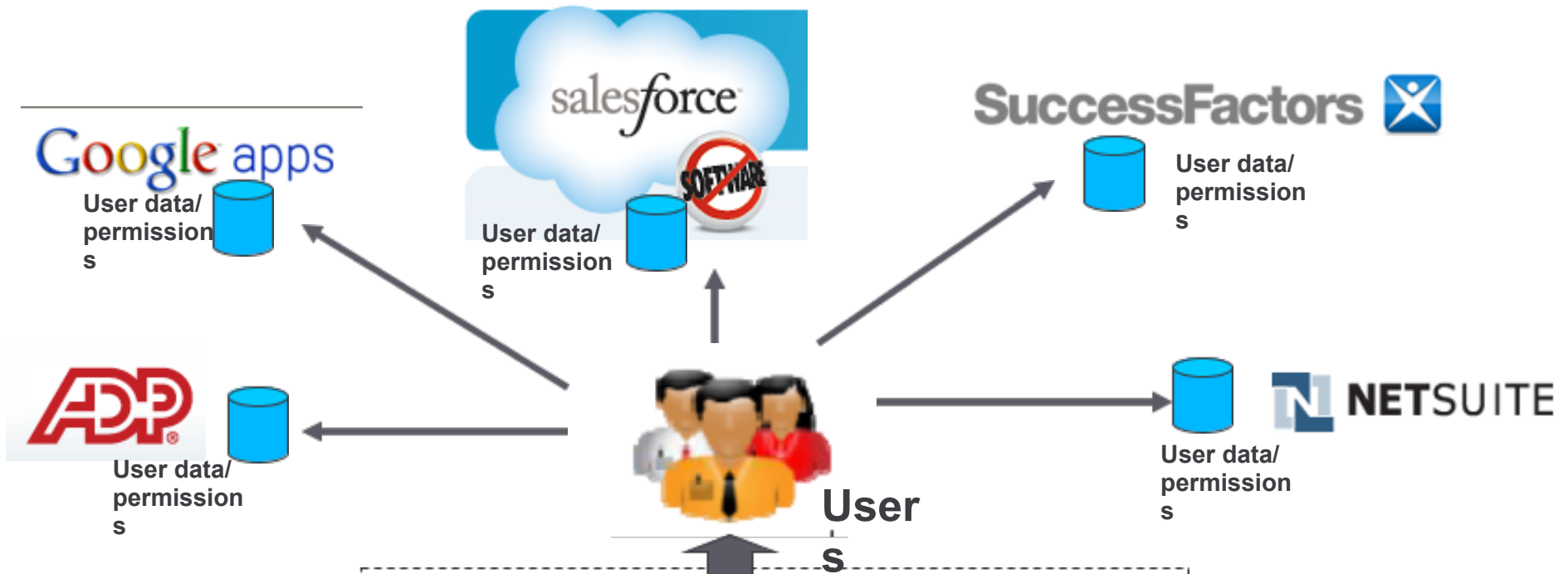
Figure 2. Total Software Revenue Forecast for SaaS Delivery Within the Enterprise Software Markets, 2007-2012



Source: Gartner (August 2008)

With CRM and Content/Communication and Collaboration leading the way...

# Creating IT Administration Nightmare



## Enterprise Challenge

- Multiple Username/ passwords
- Multiple identity silos
- Disparate administration tools
- Challenge in timely de-provisioning accounts of ex-employees

# Real Quotes on Concerns over Security

- **DuPont**, “When a sales person leaves the company, it takes 10 days to de-provision their account in Salesforce.com. Until then, the sales person has access to his account. This is a real problem.”
- **International Fragrances & Flavors**, at an executive briefing, told us, “We cannot use SaaS until it uses our identity management systems.”
- “What’s keeping us from getting more large enterprise customers? Trust.” – David Carroll, **Salesforce.com** evangelist

# Breaking down security concerns

## Trust

- Identity, authenticity
- Monitor, enforce compliance
- Multiple identities in the cloud
- Trustworthy hosted resources

## Manageability

- Provisioning users and tenants in a hosted environment
- Roles-based access
- Policy-driven management
- Intelligent workload management

## Accessibility

- Physical data location
- Physical security

## Financial

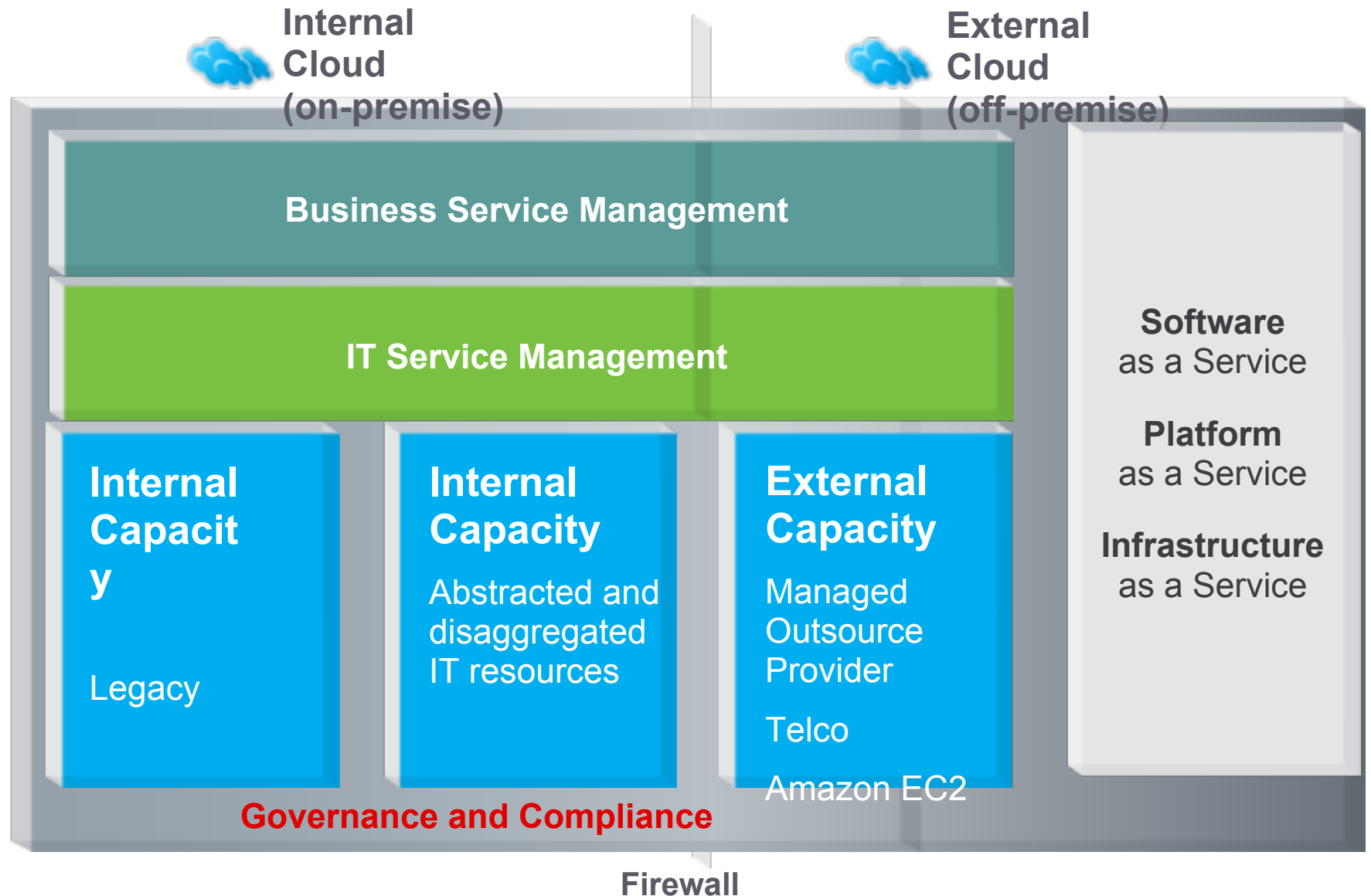
- Audit, logging, reporting
- Cost to refactor traditional applications
- Re-purpose existing resources in the data center

## Contractual

- Compliance violations
- Business service mgmt
- SLAs, e.g., 99.99% uptime
- Intellectual property issues
- Meeting GRC regulations in the cloud

What do Enterprises want you to do?

# Enterprises want to attach the same Governance and Access Policies to the Cloud as they have internally



# 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)


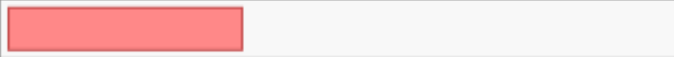




Response	20%	40%	60%	80%	100%	Frequency	Count
Single sign-on						54.2%	45
<b>Audit tracking in SaaS</b>						<b>55.4%</b>	<b>46</b>
Provisioning of users to SaaS application						48.2%	40
Support for multiple security standards (SAML, WS-FED, etc.)						18.1%	15
Multi-factor authentication						26.5%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

- Audit tracking, Single sign-on and Provisioning of users were the three main security capabilities customers are asking SaaS providers about; about 1/2 of SaaS providers indicated customers asked them about these capabilities.

# 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
<b>Build the functionality in-house</b>						<b>34.9%</b>	<b>29</b>
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
<b>Valid Responses</b>							<b>83</b>

- 1/3 of SaaS Providers prefer to build the requested security capabilities in-house
- 1/4 indicated they would prefer to OEM from a third party vendor and another 1/4 indicated they would prefer to source as part of their hosting environment.

What can cloud vendors do?

# Vendors

- SAS 70
- Identity protection and user-controlled access/authorization
- Audit/GRC
- Transparency
- Join the Trusted Cloud Initiative

# SAS 70 Certification

- Created by American Institute of Certified Public Accountants
- *“Represents that a service organization has been through an in-depth audit of their control objectives and control activities, which often include controls over information technology and related processes.*
- Independent “service auditor” issues opinion on servicer’s controls, useable by servicer and their customers
- Type I: a snapshot on a specific date, self reported
- Type II: Opinion delivered about ongoing controls

# Identity Protection

- What is the process for
  - Provisioning identities?
  - Guarding them?
  - De-provisioning with role changes?
- Does vendor support multi-factor authentication?
- Do they support standards-based federation?

# Audit/GRC

- How do you find out what's going on inside your vendor's data center?
- How do you check up on SLA terms?
- Can you reconcile information you do receive with the rest of your GRC inspection regime?
- Is sensitive data exposed in the cloud?

# Transparency issues

- Who can reach data?
- What level of encryption is available? Practical?
- Where is data located?
- Where is compute located?
- SLA terms (Microsoft requires an NDA to even see their SLA model agreement!)

# Responsibility

## Trust

- Identity, authenticity
- Monitor, enforce compliance
- Multiple identities in the cloud
- Trustworthy hosted resources

## Manageability

- Provisioning users and tenants in a hosted environment
- Roles-based access
- Policy-driven management
- Intelligent workload management

## Accessibility

- Physical data location
- Physical security

## Financial

- Audit, logging, reporting
- Cost to refactor traditional applications
- Re-purpose existing resources in the data center

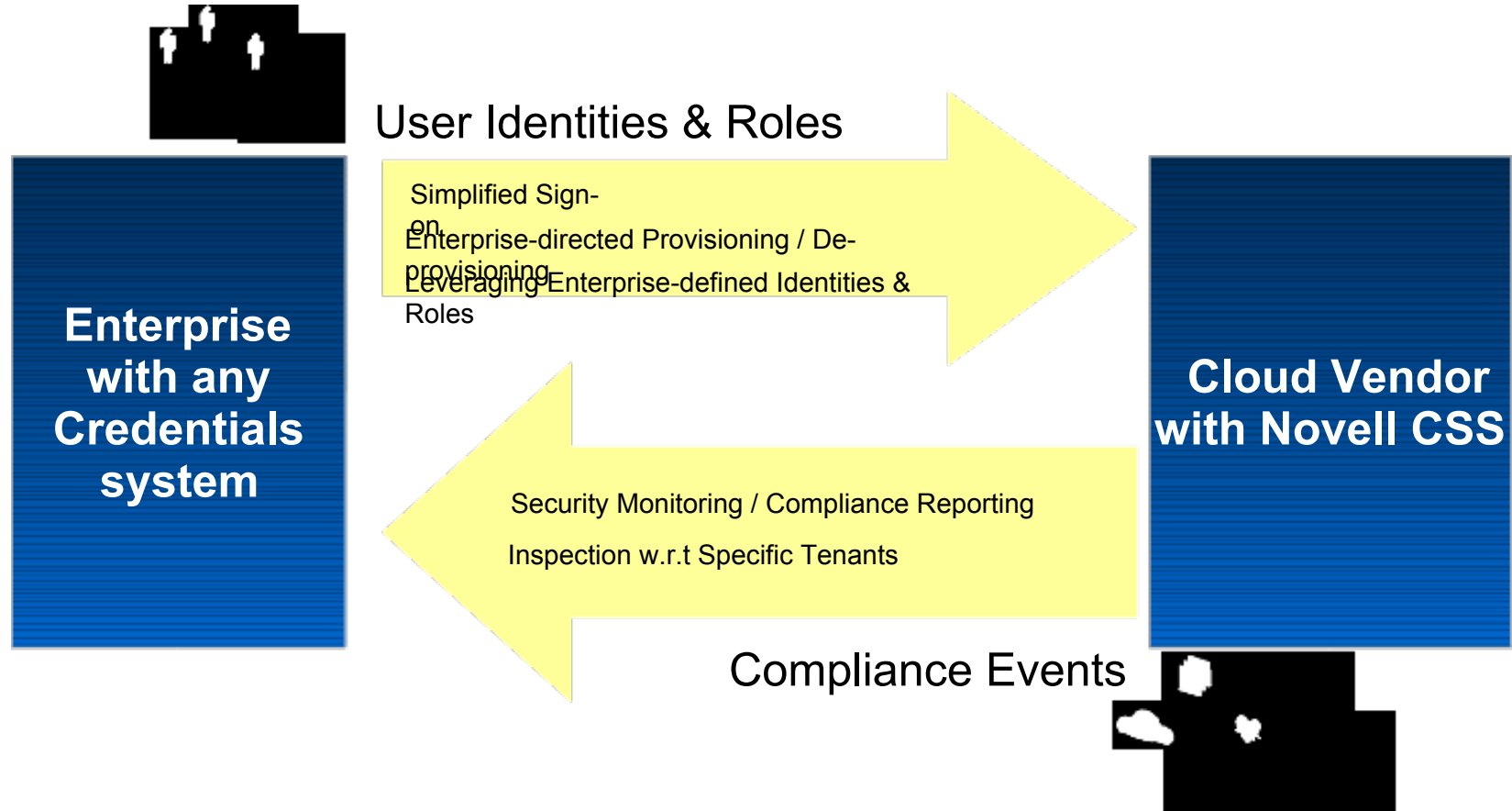
## Contractual

- Compliance violations
- Business service mgmt
- SLAs, e.g., 99.99% uptime
- Intellectual property issues
- Meeting GRC regulations in the cloud

Vendor **Enterprise** Joint

# Novell Cloud Security Service (NCSS)

NCSS is a multi-tenant identity and access solution that leverages an enterprises existing identity infrastructure to securely access SaaS applications. NCSS provides your customers with single sign-on, detailed audit logs and is built on industry standards.



# Trusted Cloud Initiative

- Cloud Security Alliance and Novell are jointly pursuing an initiative to create the industry's first cloud certification criteria.
- For more information, logon to [www.trusted-cloud.com](http://www.trusted-cloud.com)

Come see a live demo of Novell Cloud Security Service  
at the Novell Booth!

# Cloud Security Q&A

