Symplified The Cloud Security Experts

Building The Business Case For Symplified SinglePoint

Talking To Your CFO About The Benefits Of Symplified Cloud Security

Building The Business Case For Symplified SinglePoint

Talking To Your CFO About The Benefits Of Symplified Cloud Security

Table of Contents

The Business Case for Symplified SinglePoint

Talking To Your CFO About The Benefits Of Cloud Security

Introduction

Cloud computing is here stay. Organizations around the world have recognized that cloud computing, when properly applied, can bring substantial operational and business benefits to the bottom line. Applications that were once run on-site have now found a home in the cloud where maintenance and updates occur automatically; allowing businesses to focus on their core market opportunities instead of IT tasks. The cloud allows administrators to enable access for users immediately as their needs require since the applications are easily accessed through a web browser.

> Nearly every company is already using the cloud to some degree or another. Web-based email technologies deployed from the cloud is commonplace. Other companies have been using online CRM applications for years now. Businesses have recognized that while many applications are business critical, they don't need to be deployed on the business's premises and actually perform better online. The trend towards more cloud computing is accelerating, with the migration of many business processes across the firewall, including HR (e.g. Workday), payroll (e.g. ADP), and sales force automation (e.g. Salesforce.com). Collaboration is advancing as businesses move content and applications from their local premises to the cloud (e.g. Google Apps).

Although the cloud promises to reduce costs and make computing easier for companies, it is not without its challenges. Organizations continue to be concerned about its general security and the location of their data not being housed within the business. Many companies are unwilling to open up their networks and move data to the cloud due to fears that their data isn't as secure as if were inside the firewall behind perimeter controls.

The cloud's ability to provide "anywhere access" is a double edged sword. Its convenience for users and administrators is unmatched, revolutionizing the capabilities of remote workers. However, because user-to-app access occurs outside the corporate firewall, the most prominent component of IT security for past 15 years – the firewall – is of little use. Companies must carefully review their current security model in light of the cloud and understand where new vulnerabilities and silos may exist.

> For example, with multiple cloud applications in their use, companies often end up with silos of security; managing identity access separately for each application, with little ability to track and audit access rights and activity for the same user across different apps. Managing multiple silos of identities is time consuming and opens up greater opportunities for unauthorized access. Additionally, with user access to the cloud across an enterprise means companies will have more difficulty demonstrating compliance.

As the perimeter continues to disappear, identifying solutions to cost effectively manage access from the network up to the cloud is paramount. For many companies, identity and access management (IAM) is still a costly and difficult challenge and the legacy approach of one-to-one integration has fallen short on delivering lasting results. What's required to address this challenge is a cost-effective and secure fabric between the enterprise and the cloud where administrators have centralized identity administration; and completely auditable. In short, enterprises are seeking an identity access management fabric that provides strong access controls, simple single sign-on, centralized and consolidated user management, and complete auditing and reporting functionality.

The Cost Benefits Of The Cloud Model

With enterprises scrutinizing every IT expense, it makes sense to look at each facet of cloud expenditures to see where the benefits, costs, and challenges lie. What many executives find compelling about the cloud are the enormous costs savings. These savings can be found across all tiers of the cloud from the applications (SaaS), the platforms (PaaS) and the infrastructure (IaaS).

Software-as-a-Service

Software-as-a-Service apps like Salesforce.com provide rich enterprise-class CRM and SFA capabilities at roughly $50/user/month. When you factor in the savings of not licensing expensive on-premises software like Siebel/Oracle, the hardware, the data center resources and IT support, many enterprises are finding they are saving more than 70% when compared to the in-house approach.

Platform-as-a-Service

Using the cloud as an app development platform, such as Google's App Engine or Microsoft's Azure, results in significant cost savings that are nearly impossible to achieve with in-house options. Consider the price of 'free' with Google – you can serve 1,300,000 Web requests per day for free and if you exceed that quota, the costs are measured in cents per gigabyte of traffic. With low costs like these, and adequate security and integration in place, it's only a matter of time until most companies will be using the cloud for app development.

Infrastructure-as-a-Service

Using a cloud-based infrastructure, enabled through hypervisor virtualization, is the third major area of cost savings. With Amazon's Elastic Compute cloud (EC2), enterprises can obtain burstable virtual machines using Linux or Windows at an amazingly low cost. Today, it costs only $0.085 per hour to use a Linux server hosted at Amazon. Using Amazon's database service in the cloud is free for the first 25 hours every month and thereafter only 14 cents per hour. Providing that level of availability and elasticity on-premises would cost several times as much and require an extremely sophisticated IT team's full-time attention.

The cloud offers any user or developer the benefits of subscription, pay-as-you-go model. Instead of carrying a capital asset on your books for hardware, you pay only for the services when needed. Traditional on-premises deployments require large up-front payments for hardware and software; not to mention the staff that needs to be hired and trained to support the rollout and ongoing maintenance.

The cloud model maintains the software and has trained experts who are responsible for your application's ongoing upkeep 24X7. Anytime there are software updates, your user gets the latest upgrade and patches as part of the subscription. If you no longer need the service you can turn it off or scale back.

The Costs Of Cloud Identity & Access Management

There is no question that provisioning users and managing access takes time and money whether you are accessing the cloud or not. And the software cost is just the tip of the iceberg. Companies that have implemented traditional identity and access management software typically spend three to five times the cost of the original license for customization, training and ongoing product support according to Gartner.

You can also look at the cost of traditional provisioning. There have been many studies conducted on how much it costs to add a new user and the time it takes to fully grant access to all the disparate systems they need on the network. It's not uncommon for provisioning to take some larger companies up to 30 days to provide all the needed access. That's nearly a month of impaired productivity whenever a new employee joins the company.

The sheer number of user accounts has never been greater. Consider that each new cloud app has its own user database or directory. Each user has an identity in that database. As more cloud apps are adopted the number of user accounts scales linearly and sometimes geometrically. One Symplified customer, for example, has 2,500 employees and uses 14 cloud apps resulting in nearly 35,000 identities that must be managed at significant cost. Now as they extend more applications to their customers, that number is ballooning to the hundreds of thousands; the number of managed accounts is overwhelming. Further compounding the management challenge is that these credentials are scattered all over the cloud resulting in a hundredfold increase in attack vectors and account hijacking risk.

Should You Build or Buy An IAM Solution?

Some companies may still be thinking that they can develop an adequate identity access management (IAM) solution on their own. But they often discover that the task is enormous and even deciding on an adequate feature set can take months. Companies could easily spend $1 million or more and spend a year and half of development to only build a partial IAM solution. Other enterprises think that open source IAM is the way to go. However, the open source option requires heavy customization and development effort to integrate into your network environment.

The ongoing costs to support such solutions can also be significant. If a company downsizes or loses the talent that built the application, they are faced with a real 'identity' crisis and may be forced to abandon their home grown solution.

Forrester estimates that a typical IAM project's first phase can easily cost half a million dollars, including implementation services and licensing costs.[1]

Organizations also look at solutions from commercial IAM platform vendors, but contrary to their marketing claims these products are the result of many acquisitions that have not been integrated. The customer is left to integrate each IAM module and then connect into the infrastructure of directories and web apps in a painstaking process. The bottom line is that building an IAM solution is not a viable option for companies. Buying a commercial on-premises product is not much better as the integration effort is still significant and complex.

Typical Costs of Commercial IAM Implementation*

Federation:	
Web Access Management:	**$211,000**
User Provisioning:	**$175,000**
Virtual Directory:	**$360,000**
User Directory:	**$100,000**
Cost to integrate WAM With Web App (per application):	**$110,000**
	$50,000

*Forrester Research

The following survey results point to the difficulties when deploying a typical IAM solution:

Fifty-eight percent of companies surveyed by Ponemon Institute report using mostly manual processes for monitoring identity controls.[2]

Maintenance and support fees add another 20% annually. A company will essentially pay for their license again about every five years.

Only 13 percent of companies surveyed by Ponemon Institute describe their company's approach to identity compliance as centralized.

IAM upgrades are expensive to do and companies have to handle them on their own as it involves updating an agent on a workstation, for example.

With the advent of the cloud, IAM solutions are now available through the cloud (Identity-as-a-Service) and provide a superior alternative, just like other cloud applications, to reduce your user management costs. Cloud-based IAM solutions provide all the same cost and agility benefits of other cloud applications without the hassles of implementing your own IAM infrastructure. Forrester conservatively estimates that IAM delivered on-demand saves 30% to 40% compared to licensed on premises software.[3]

Calculating Cost Savings, ROI & Payback Periods With SinglePoint

Implementing an IAM solution has proven quantifiable benefits. Just a simple password reset for any of the many applications that a user has access to can require a help desk's time, adding tens of thousands of dollars in administrative expense each year to a company's IT budget. Using the widely known Forrester Research ROI model for SSO you will see the positive ROI impact that implementing SSO can have.[4] Then when we substitute Symplified's subscription model instead of legacy software you can see how the ROI and payback periods dramatically improve.

Legacy SSO Software

[4] Forrester Research

Benefits

			Monthly	Yearly
Recurring	Help Desk		$ 36,667	$ 440,000
	IT Administration &Audit		$ 25,750	$ 309,000
		Total	$ **62,417**	$ **749,000**
Non-recurring	Two-factor Authentication - Integration Savings			
				$ 200,000
		Total		$ **200,000**

Costs

Initial Costs		**Total**		$ **890,865**
Recurring Costs	Ongoing Administration		2hrs /mo.	$ 1,800
	Annual Software Maintenance Fee		18%	$ 135,000
	Annual Server Hardware Maintenance Fee		18%	$ 5,760
		Total		$ **142,560**

ROI

	Year 1	Year 2	Year 3	Total	PV
Total Benefits	$ 949,000	$ 749,000	$ 749,000	$ 2,447,000	$ 2,447,000
Total Costs	$ 1,033,425	$ 142,560	$ 142,560	$ 1,318,545	$ 1,164,403
Net Yearly Savings	$ (84,425)	$ 606,440	$ 606,440		
Total Net Savings	$	$ 522,015	$ 1,128,455	$ 1,128,455	$ 808,067
			Payback Period (Months)		**13.1**
			Return ON Investment (ROI)		**76%**

Symplified SSO Subscription

Benefits

			Monthly	Yearly
Recurring	Help Desk		$ 36,667	$ 440,000
	IT Administration &Audit		$ 25,750	$ 309,000
		Total	$ **62,417**	$ **749,000**

Costs

Initial Costs	Initial Symplified CAM SSO Deployment (10,000 Users)			$ 150,000
	CAM Subscription			
Recurring Costs	Identity Router Subscription		$ 7,000	$ 84,000
			$ 1,500	$ 18,000
		Total	$ **8,500**	$ **102,000**

ROI

	Year 1	Year 2	Year 3	Total	PV
Total Benefits	$ 749,004	$ 749,000	$ 749,000	$ 2,247,012	$ 2,045,851
Total Costs	$ 252,000	$ 102,000	$ 102,000	$ 456,000	$ 381,246
Net Yearly Savings	$ 497,004	$ 647,004	$ 647,004		
Total Net Savings		$ 1,144,008	$ 1,791,012	$ 1,791,012	$ 1,664,605
			Payback Period (Months)		**Less than 2 mo.**
			Return ON Investment (ROI)		**437%**

5.75x ROI than software.

Payback less than 2 months!

Using Forrester Research's model you can see that not only does SSO pay for itself quickly, but when you analyze the low-cost subscription model that SinglePoint provides the ROI increases from 76% to 437%, more than 10X improvement and payback period decreases from 13.1 months to 1.8 months for an improvement in payback period of more than 5.75X. The lower initial and on-going costs involved with a subscription model are significant in turbo charging ROI with a lower TCO.

Nothing conveys the value of the IAM project better than its contribution to reduced call center costs due to fewer helpdesk calls, fewer audit findings — and thus lower cost of mitigation of audit findings around user access recertification. An additional benefit is improved productivity of adequately provisioned users (having all access to applications when they start versus having to wait two to three weeks for all access to be granted).[5]

Cost Advantages Of On-Demand Vs. Software-Delivered IAM Models

The on-demand IAM model is gaining traction for the same reasons that other cloud applications are also rising in popularity. With a cloud-based IAM solution, executives can run a pilot phase to measure the benefits of their IAM deployment from the cloud. Organizations can achieve significant cost savings by using a hosted IAM solution versus building it in-house with software. The following table[6] illustrates a comparison between to two IAM models and how your costs will vary.

Resource Type	Infrastructure Software Model	On-Demand Model
Software Cost	Requires upfront payment of software licenses and support	Pay only for the number of licenses that you need, add more later, no support expense
Hardware	Requires purchase of hardware including servers, workstations, networking devices and mobile devices	No servers, workstations or networking devices need to be purchased
People	A typical organization of 1000 employees requires 3-4 staff to support the IAM project plus consultants	Maximum 1 FTE to oversee operations, possibly a consultant for initial assistance and training
Integration Time	9 to 12 months	1 to 3 months

Cost Advantages Of Integration Hub Vs. One-to-One Federation Models

A research project conducted by the Burton Group placed the cost of deploying a federated SSO solution at a minimum of $250,000 per year. Those companies daring enough to attempt to build their own federated SSO solution will need the following:[7]

- ✔ A business case
- ✔ A project manager
  - » For central services
  - » For each federated connection
- ✔ At least four FTEs, including software developers
- ✔ Convenient access to a lab that approximates your environment and your partners'
- ✔ Budget for software and maintenance
- ✔ Could go open source, but then more development time

SinglePoint's breakthrough integration hub model radically redefines the cost economics of federation by changing the fundamental equation. With the expensive, complex one-to-one federation model each SAML connection must be established on a one-by-one basis, a model that can be expressed as (enterprise x application) or (e x a). This model means that each new connection, results in linear or geometric growth in cost due to integration friction.

Symplified has revolutionized the model for integration using our iTunes-like delivery architecture through a hub-spoke design. This one-to-many approach changes the equation to (enterprise + application) or (e + a), resulting in a constant rather than linear equation translating to 85% lower costs. Federate software products are expensive capital investments. Perhaps most important in an SSO solution is its app coverage – SAML is limited to just 5%[8] of all apps whereas Symplified not only supports SAML but also through HTTP-FED can support the critical other 95% of apps. The following table[9] illustrates a comparison between to two federation models and how costs will vary.

First Generation Federate Software	Cloud-Generation Federation Service	Benefit
Base software cost $50,000 per server servicing 2,500 users and 5 apps	No software licensing needed	Save $50,000 per software server
Fail-over server software license (50% discount) $25,000 per server	Built-in redundancy in SinglePoint Trust Cloud	Save $25,000 per fail-over software server
Federation Connection licenses $15,000 each	No per connection license needed	Save $75,000 for 5 federated connections
Federation services integration expense between both organizations 3 business days (24 hours @ $175/hour = $4,200) each	Activation model – 5 minutes of configuration	Save $21,000 in integration expense for 5 apps
Integration with non-SAML apps is impossible	Integration with any Web app is possible with HTTP-FED	One SSO solution for both SAML and HTTP Web apps
20% annual software maintenance expense $30,000 per year	Support and upgrades built into subscription	Save $30,000 in first year support contract
First year costs using Federate software for 5 SAML apps with fail-over configuration = $201,000	Cost for 5 SAML apps, 2,500 users using SinglePoint ConnectExpress = $30,000 Save $171,000 or 85% lower costs	**Save $171,000 or 85% lower costs.** **Deploy in a fraction of the time without learning curve of SAML**

SinglePoint Provides Unified Security For Both the Enterprise & The Cloud

The SinglePoint platform links your existing security infrastructure securely to the cloud. This technology allows you to implement a powerful, cost effective IAM solution where internal and external users can gain single sign-on access to your cloud applications as needed. Only Symplified offers a truly integrated, yet modular, IAM stack unifying Web Access Management, Cloud Access Management, federation, SSO, lightweight virtual directory and auditing for both on-premises enterprise and Cloud apps. Unlike software focused solely on-premises, SinglePoint provides a unified solution capable of meeting your IAM challenges across enterprise, SaaS and Cloud platforms.

SinglePoint's rapid innovation cycle delivers new capabilities quickly, while platform vendors roll out new releases only every 18 months, often requiring painful "forklift" upgrades. SinglePoint includes automated upgrades, ensuring you are always on the latest, most secure version without disrupting your operations. The following table illustrates the key functionality of the SinglePoint platform and the benefits provided through this innovative technology.

Key Functionality	Benefit
Extend user access beyond the network	Allow users, partners, and customer secure access to cloud apps
Extend policy from the enterprise to the cloud	Re-use your existing security infrastructure/ keep credentials safely behind your firewall
Full audit logging	Enhance your security and compliance efforts through complete audit logging of all administrator and user activity
Centralized management	Manage both cloud and enterprise web application access. Add/remove users quickly and easily
Consolidate identities and directories	Increase security and reduce administrative burden by consolidating identities and directories
Flexible access management	Assign users different levels of access to applications
Manage multiple cloud apps	Save time and reduce administrative burden
Scalable IAM	Scale beyond pilot deployments, increase user counts and adoption, accelerating ROI of cloud app investment

How Does Symplified Meet Business Objectives?

One of the most important questions a company must ask when selecting an IAM vendor is: "Does this solution meet our business objectives?" SinglePoint meets business objectives across four key areas:

1. Enable cross-cloud collaboration, mobility and externalization of internal apps
2. Streamline IT infrastructure and operational costs
3. Improve business outcomes and results
4. Deliver Forrester Research's 5 R's of Information Security

SinglePoint Enables Cross-Cloud Collaboration, Greater Mobility & Externalization Of Internal Apps

The SinglePoint platform was specifically designed to enable enterprises to leverage the Cloud as a low cost yet secure collaboration platform that crosses organizational boundaries and firewalls. With the ability to rapidly set up collaboration environments while maintaining security and trust throughout, enterprises can achieve cost savings, create new products and accelerate time to market. Some examples:

- Collaborate across corporate firewalls with 3rd parties, suppliers and clinical research partners
- Collaborate with Joint Venture (JV) partners for short term and medium term collaborations quickly
- Integrate with suppliers across the value chain to provide access to internal apps and access apps of your partners
- Streamline R&D efforts leveraging specialized capabilities and apps of your partners
- Provide direct access to apps by your channel and distribution partners
- Provide mobile access to enterprise apps and Cloud apps to support an increasingly mobile workforce that requires global secure access
- Externalize internal apps like SAP, SharePoint, Oracle and others to accelerate business velocity

SinglePoint Improves Business Operations.

As mentioned at the beginning of this paper, companies that are outsourcing applications to the cloud are looking to offload certain IT activities to an entity best-suited for that task. This allows companies to focus on their business rather than on IT. SinglePoint helps companies move business processes securely across organizational boundaries.

Symplified SinglePoint meets the business objectives of companies who want to reduce their operational costs, improve their business operations, and increase the success rate of their SaaS and cloud roll-outs. Companies that were once concerned about how to manage access to cloud applications can now utilize the SinglePoint solution to:

- Scale the number of users in a particular SaaS app as pilots prove out and need to expand to large scale production deployment.
- Scale the number of SaaS and cloud apps in use as cloud becomes more central to the enterprise IT strategy
- Enable the enterprise to roll out more cloud and SaaS apps quickly thereby benefiting more quickly from those apps' ROI benefits

SinglePoint Secures, Integrates & Extends Existing IT Infrastructure.

SinglePoint meets your IT requirements in a numbers of ways. Perhaps most significantly is that this platform integrates with your existing network systems. There is no need to undergo expensive migration or consolidation projects to replace directories or rip out existing infrastructure. SinglePoint uses advanced virtualization capabilities to unify all internal and external identity components, such as LDAP, Active Directory or other repositories, and applications without agents, leaving the data and system in-place. SinglePoint:

- Provide access management, authentication, SSO, federation, auditing, compliance and administrative capabilities
- Integrates behind-the-firewall the security infrastructure with the cloud
- Virtualize and integrate disparate elements of the enterprise security and identity infrastructure
- Streamline enterprise identity management by breaking down security management silos
- Improve security and simplify compliance reporting
- SinglePoint is a unified solution that works across all major enterprise and cloud platforms:
  - SaaS apps such as Salesforce.com, Google App, WebEx, ADP, Concur
  - Cloud platforms such as Microsoft Azure or Force.com
  - Infrastructure-as-a-Service like Amazon EC2, Rackspace Cloud and others
  - In-house web apps and portals like SharePoint and SAP

SinglePoint Reduces Costs Associated With IAM.

The SinglePoint platform reduces operational costs by helping organizations manage their existing identity resources more efficiently. The following table demonstrates how SinglePoint compares to traditional on-premises IAM software solutions.

Reduce Operational Costs	Traditional Web Access Management	SinglePoint Web and Cloud Access Management
Licensing costs	Heavy initial licensing costs	Subscription pricing, no up-front licensing costs, reduces your costs by thousands
Maintenance and support	Typically 20% or more per year	No annual support fees, immediately saves you 20%
Integration Expense	Heavy integration expense for each application	Packaged apps provide integration to many applications including Salesforce, SAP, PeopleSoft saving hundreds of thousands in connector fees
Data Center Spend	Additional dedicated servers required for a comprehensive access management solution	A single 1U appliance reduces rack space, cuts power costs
Directory Consolidation	Additional redundant directories	Built in virtual directory eliminates the need for multiple directories
Staff Usage	Often requires additional staff to manage the WAM solution	Optimizes existing staff because so much of the manual effort is removed

Symplified Delivers Business Value From Information Security.

Forrest Research recommends articulating security's value by using one or more of the five R's of an effective risk management program.[10] Symplified provides value for each of these 5 R's:

1. Reputation
2. Regulation
3. Revenue
4. Resilience
5. ROI

Reputation:

Protecting brand equity is an increasingly difficult challenge. Symplified provides a simple solution for protecting against an increasingly complicated internal and externl threat paradigm. Since collaboration across organizations is increasing, the protections Symplified provides mitigates abuse or misuse of data from both internal and external users.

Regulation:

Symplified security reduces the costs of meeting IT and regulatory mandates. Symplified allows organizations to comply with multiple regulations effectively especially as data moves outside the firewall into disparate silos. With Symplified you can meet compliance requirements, avoiding fines or penalties enabling a move towards a sustainable risk management strategy.

Revenue:

Symplified security protects existing revenue streams and helps generate new ones. Symplified protects against the loss, theft or disclosure of critical data including sales, customer, financial and personnel data in apps both inside the firewall and in the cloud. A better user experience, through the SSO and personalization that Symplified provides, can be a significant differentiator from your competitors online. Aggregating multiple SaaS and enterprise apps through a Symplified portal creates new revenue sources by reselling access to multiple apps.

Resilience:

Symplified security ensures business function during adverse conditions like natural disasters. Because Symplified is optionally delivered through the cloud it comes with built-in geographic redundancy that often is more robust than what can be provided on-premises. Symplified enables enterprises to adopt more cloud apps which themselves also have greater availability and redundancy than on-premises software resulting in overall greater availability and resiliency to disaster.

Return on Investment:

Security affects both the top and bottom lines of the business. The collaboration capabilities that Symplified enables deliverer new efficiencies realized across business processes resulting in improved business outcomes. With the user experience and SSO simplicity that Symplified provides, organizations can leverage the cost saving benefits of SaaS apps more broadly across the enterprise delivering greater ROI of multiple SaaS apps. Symplified's subscription service enables enterprises to avoid spending capital on software and move to predictable subscription models. Symplified can directly reduce operational expenses by streamlining helpdesk and account management expenses.

Summary

The benefits of the cloud are significant and most companies are embracing the cloud to some degree already with Web-based applications and business process solutions. As companies adopt more cloud-based applications, the task of managing identity and access becomes more complex, time consuming, and risky. Compounding the issue is that many organizations have had difficulty deploying an IAM solution that meets their needs and within a reasonable budget.

SinglePoint meets your business objectives by offering a powerful cloud (and appliance-based solution) that provides single sign-on, identity management and centralized control for multiple cloud applications. SinglePoint meets business needs cost effectively at 50-85% lower costs, allowing enterprises to focus on their core competencies rather than losing focus on the ongoing challenges of achieving pervasive security.

About Symplified | The Cloud Security Experts

Symplified provides the Trust Fabric of the Cloud – integrating enterprise security policies and administration with cloud applications and data. The SinglePoint solution is available either as an on-premises appliance or delivered from the cloud as a secure proxy. SinglePoint is pre-integrated with leading cloud applications and platforms including Google Apps, Salesforce.com, ADP, Taleo, Xactly, Jive, Workday and many others. Symplified's founding management team also created Securant and the ClearTrust product, which pioneered the market for Web access management, provisioning and federation software. Securant was acquired by RSA Security for $140M. Venture funding for the company was provided by Granite Ventures and Allegis Capital.

Symplified is headquartered in Boulder, Colo., with offices in Palo Alto, Calif.
Visit us on the web at www.symplified.com.

References

[1] Hosted Identity is Real: Are you Ready for It?, Forrester, 2009

[2] Survey on Identity and Compliance, The Ponemon Institute, 2007

[3] Best Practices: Identity Management in the Could, Forrester 2009

[4] Justifying E-SSO: Benefits Beyond The Help Desk - Identity Management And Security That Makes Users' Lives Easier by Jonathan Penn

[5] Identity And Access Management Mitigates Risks During Economic Uncertainty, Forrester 2009

[6] Hosted Identity is Real: Are you Ready for It?, Forrester 2009

[7] Federation's Future in the Balance: Teetering Between Ubiquity and Mediocrity, Burton Group, 2007

[8] Forrester Research, The State Of Federation by Andras Cser

[9] Hosted Identity is Real: Are you Ready for It?, Forrester 2009

[10] Forrester Research, Articulating The Business Value Of Information Security by Khalid Kark