

The Business Value of Internet Identity Security

Executive Overview

Internet Identity Security products like Ping Identity's® PingFederate® and PingConnect™ provide Internet Single Sign-On, Automated Internet User Account Management and Identity-Enabled Web Services capabilities¹. These capabilities translate into direct business value by increasing end user productivity, increasing Internet application adoption rates, decreasing administrative overhead, decreasing help desk costs and increasing the security of Internet applications such as Software-as-a-Service (SaaS). Internet Identity Security products also assist in regulatory compliance initiatives by providing a centralized, auditable point of Internet application access control and automating the management of Internet user accounts.

This paper illustrates how deploying Internet Identity Software can result in a 100% payback on the first-year investment in only four months with full payback on a three year investment in only ten months, resulting in 300%+ ROI over three years. As your needs grow, so do the business benefits, as Ping Identity's solutions deliver even more value as additional users and Internet applications capitalize on economies of scale within the solution.



1 PingFederate only

Table of Contents

1 Introduction.....	3
2 The Business Value of Internet Single Sign-On.....	4
2.1 Business Benefit #1: Decreased Help Desk Costs.....	5
2.2 Business Benefit #2: Increased Application Adoption Rate.....	6
2.3 Business Benefit #3: Increased Employee Productivity	6
2.4 The Total Business Benefits of Internet SSO	8
3 The Business Value of Internet User Account Management.....	8
3.1 Business Benefit #1: Decreased Administrative Overhead.....	9
3.2 Business Benefit #2: Reduced Risk of Data Theft and Unauthorized Account Access	9
3.3 Business Benefit #3: Increased Compliance Audit Pass Rate...	10
4 The Business Value of Identity-Enabled Web Services.....	10
5 Internet Identity Security ROI	11
5.1 Return on Investment (ROI).....	11
5.2 Net Present Value (NPV)	12
5.3 Time-to-Value (TTV) and Payback Period.....	12
5.4 Total Cost of Ownership (TCO)	13
5.5 An Example PingFederate Internet Identity Security ROI Calculation.....	13
5.5.1 Total Cost of Ownership.....	13
5.5.2 Business Benefit Calculations	14
5.5.3 Internet Identity Security ROI and Payback Calculations	14
5.5.4 Calculating Net Present Value and Risk-Adjusted ROI....	15
6 Conclusion	16



1. Introduction

Today's business climate is tough. The ongoing recession has driven virtually every dollar of Capital and Operational Expenditures (known as CapEx and OpEx henceforth) under a financial microscope. Prospective IT investments must be reinforced with a strong business case in order to gain approval, and those that demonstrate a high return on investment (ROI) coupled with a rapid payback yield great benefits for the organization in a short period of time. From a CFO's perspective, investment decisions must be made analytically, comparing the return from any given investment against alternate investments, including doing nothing (such as leaving the cash in the bank).

One investment that consistently yields high rates of return is Internet Identity Security, which provides substantial business benefits including reduced expenditures, increased employee productivity and decreased risk. In partnership with a best-of-breed vendor and technology, returns can be realized in a very short period of time, eclipsing many other investments.

This paper demonstrates how PingFederate and PingConnect, Ping Identity's flagship Internet Identity Security products, provide substantial and quantifiable areas of business value:

1. Internet Single Sign-On
2. Internet User Account Management
3. Identity-Enabled Web Services²

Internet Single Sign-On (SSO) allows personnel to access Internet applications including Software-as-a-Service (SaaS) and Business Process Outsourcing (BPO) applications without requiring additional logins beyond the user's initial network sign-on. While application outsourcing provides many business benefits including CapEx reductions, it can also drive up OpEx by requiring more administration and exacting productivity "taxes" due to repeated application logons, password resets and help desk calls. Internet SSO eliminates much of this overhead, increasing the overall ROI of outsourced applications. Internet Because Internet SSO removes barriers to using Internet applications, it also increases user adoption rate—in some cases dramatically.

Internet User Account Management reduces administrative overhead from Internet application deployments. When an application is outsourced, "remote" accounts are created for each employee that requires access to the application. While this overhead is insignificant with only a few users, costs rapidly spiral out of control when deployments grow into the hundreds or thousands of users. Internet user accounts must also be managed in a timely fashion to ensure that changes in employee status are quickly replicated to the Internet application user directories. Failure to do so can result in unauthorized application access, data loss and compliance issues.

Identity-Enabled Web Services³ support the "next generation" of Web application architectures. As Internet applications become increasingly distributed and the adoption of Web Services and Service Oriented Architectures (SOA) become more prevalent, the need to share user identity beyond the Web server has become a business enabler. Identity-Enabled Web



² PingFederate only

³ PingFederate only

Services provide a scalable, cost effective, secure, Internet-friendly mechanism for Web Services to share identity with one another, resulting in higher levels of application security and improved user experience due to high levels of personalization.

Each of the three benefit areas outlined above will be described and quantified in detail in subsequent sections of this white paper, and the paper will conclude with specific Internet Identity Security Return on Investment and payback calculations.

2. The Business Value of Internet Single Sign-On

The concept of Internet SSO was introduced in the previous section. In addition to a highly visible benefit for end users (who love the convenience and have become accustomed to SSO for internal applications), Internet SSO delivers substantial business benefits including increased employee productivity and decreased help desk costs.

Security has always been a high imperative for IT, and with the recession in full swing the number of people that are desperate enough to resort to crime to pay the bills has been increasing rapidly. According to the Anti-Phishing Working Group, the number of active "crimeware" Web sites reached an all-time high of 31,173 in December 2008⁴, and the trend is only projected to increase. These sites use a variety of means to steal user identity, including mimicking an actual web site in order to obtain the user name and password of everyone that falls into their trap. Once the user name and password has been compromised, the criminal can steal data and potentially create irreparable harm to the organization.

When the number of applications running outside of an organization's firewall increases, so does the risk of password theft. Consider that the more distinct user names and passwords that a user must memorize, the higher the chance that they will choose easy-to-guess passwords ("password fatigue"), and that they will store those passwords where they can be stolen.

A simple and elegant solution to this dilemma is Internet Single Sign-On products that leverage the Security Assertion Markup Language, or SAML. While a thorough discussion of SAML is beyond the scope of this document, Internet SSO products that support SAML have one major advantage: the⁵ user's password never leaves the organization's firewall. SAML is based on the notion that once an application's user has been authenticated by their organization (the true "single sign-on") using whatever means the organization chooses to employ, that user's authentication is good enough for all other applications that they might access. SAML establishes a "trust relationship" between the user's organization and the application vendor, and when the user accesses the application, their identity is transparently and securely passed to the application vendor.

4 Phishing Activity Trends Report, 2nd Half 2008, Anti-Phishing Working Group, March 17, 2009

5 For more information on SAML, Ping Identity's Website (www.pingidentity.com) contains a wealth of information

What this all means is that a) the user does not sign on again to access applications; b) their identity and access information is passed securely to the application vendor, and since they are already authenticated, no password is required; and c) since there is no password required, there is no password to steal, phish, hack, etc.

While reducing security risk is a great benefit, it is also difficult to quantify. It's like selling insurance—you know you need it, you hope you never have to take advantage of it, but you intuitively know that you'd better buy some or the alternative could be devastating. In many cases, quantifying security risk is a bit like that—unless there has been a loss, it is very difficult or impossible to quantify. That said, most executives innately understand this advantage and will not require a quantification of the benefit.

The following sections concentrate on aspects of Internet SSO with clearly defined business values, which can be leveraged to build a compelling business case for Internet Identity Security.

2.1 Business Benefit #1: Decreased Help Desk Costs

One unintended side effect of application outsourcing can be increased help desk expenditures. When employees call the help desk for assistance with user name and/or password resets, the organization incurs help desk costs in addition to lost employee productivity. Also consider that some SaaS and BPO vendors charge their customers for these calls in cases where the organization's help desk does not handle application password issues. One large application outsourcer reports that they bill customers \$1M a year just for password reset issues!

There have been a number of studies over the years centered on the time spent by users to reset user names and passwords. Consider the following:

- Average users call the help desk 19 times a year⁶
- 30% of all service desk calls are password-related⁷
 - Between 3 and 6 service desk calls per user, per year, are password related
- Average cost of a help desk call: \$10 to \$31⁸ (median: \$21)

Next, a couple of assumptions:

- Average password-related help desk call: 10 minutes
- Average users call the help desk three times per year for Internet application password reset assistance. To keep things conservative, we will assume one only call per year

Quantifying help desk-related password reset costs:

- 1,000 users * 1 call/year * \$21/call = **\$21,000**

⁶ "The Cost of a Non-Automated Help Desk", Gartner, 2003

⁷ "Automated Password Resets Can Cut IT Service Desk Costs", Gartner, 2004

⁸ "Justify Identity Management Investment with Metrics", Gartner, 2004

Plus the lost user productivity from the help desk calls

- 1,000 users * 1 call/year * 10 minutes/call * \$0.61/minute = **\$6,100**

Total benefit from reduced help desk calls: \$27,100 per 1,000 users

2.2 Business Benefit #2: Increased Application Adoption Rate

A major business benefit of Internet SSO is increased application adoption rate. Many applications depend on reaching a certain user "critical mass" before they really begin to pay off. Customer Relationship Management (CRM) systems, for example, aren't terribly useful until a certain number of users are regularly entering and updating data during the course of their day-to-day duties. Internet SSO replaces one large adoption barrier, repeated application logins, with the same "click-and-work" convenience that users have grown to expect from business-critical applications.

Another example is online travel booking applications, which typically save organizations between \$10 and \$30 per booking compared with offline (travel agent) alternatives. One Ping Identity customer, ConAgra, reported an increase in user adoption rate from 11% to 81% after deploying Ping Identity Internet SSO. While they did not publish specific benefit metrics, consider 11,000 internal⁹ employees use the system and you can imagine the savings that resulted.

Adoption rate may be difficult to quantify depending on the business application. Online travel is relatively easy, as the cost savings are clear. CRM applications can be more difficult as the benefits are harder to quantify in hard dollars.

It is important to note that Internet SSO benefits both Internet application customer and vendor. While most of the benefits above have been oriented to the customer, vendors also benefit from increased adoption rate and decreased administrative costs. Customers that don't require password resets and automatically manage their own accounts definitely reduce the service provider's overhead, and many vendors today consider supporting SAML-based Internet SSO a basic business enabler.

2.3 Business Benefit #3: Increased Employee Productivity

While outsourced applications provide substantial savings to the organization, those savings can be reduced due to lost employee productivity. Assume that an average Internet application user signs on to an application three times per day, and assume that each login takes approximately five seconds to complete (assuming a successful login). While this may not seem like a lot of time, consider this:

- Three logins per day = 15 seconds per day, per user, per application
- Logins cost an organization with 1,000 users 250 minutes per day, per application (62,500 minutes or 130 work days per year, assuming 250 work days per year)



⁹ "Rearden Commerce SSO with ConAgra Case Study by Rearden", Rearden Commerce, 2007

In order to quantify the full cost to the organization, it is necessary to quantify the cost of an average worker:

- Average salary of a U.S. office worker: \$55,969¹⁰
- Average “burden” cost (benefits and other overhead): \$19,589¹¹ (35% median value)
- Average annual worker “fully burdened labor rate”: \$75,558 (salary + burden)
- Average “on the job” days/year: 250 (50 weeks, 5 days/week)
- Average hourly cost per worker: \$36.33 (75,558 / 2080)
- Average per-minute cost per worker: \$0.61 (\$36.33 / 60)

With the basic metrics above in place, calculating the total cost of lost productivity for the same 1,000 application users yields the following:

- 62,500 lost minutes of productivity per year
- Average cost per worker, per minute: \$0.61
- **Total benefit: \$38,125 in lost productivity per year, per application, per 1,000 users**

It is important to remember that many organizations have more than one application and greater than 1,000 users, and as a result this calculation will quite likely be several times greater.

If you want to add even more ammunition to the Internet SSO argument, you could calculate an average revenue figure per employee for your company (total revenue / total number of employees) and use that figure in place of the costs calculated above. Instead of calculating cost, calculate opportunity cost—the revenue that an average employee could generate for the organization if they weren’t spending time signing on to applications.

Consider the below example, which is based on a pharmaceutical company that is a large Ping Identity customer. Since this company is publicly held, the following key metric is readily available from their SEC filings:

- Average revenue per employee: \$600,000, or ~\$4.98 per employee/minute

Next, consider that the recovered time above, which otherwise would have been spent waiting for the login to complete, is instead used to generate revenue.

- 1,000 users recovering 62,500 productive minutes per year
- \$4.98 revenue per employee/minute
- Total: **\$311,250** (62,500 * \$4.98)

Even if you only assume a small percentage of the recovered productive time is applied to generating revenue, the benefits are clear and substantial. It doesn’t take a financial wizard to calculate a substantial business case for Internet SSO based on this benefit alone. Because this figure varies widely depending on the company, be cautious how you use this number. This figure, incidentally, is not used in the ROI calculations at the end of the paper.



¹⁰ United States Census Bureau American Community Survey, 2007, page 18

¹¹ John Hopkins University Study, <http://www.jhu.edu/ohia/burden.html>

2.4 The Total Business Benefits of Internet SSO

If you add up all of the benefits above, setting aside the increased revenue calculation, the business value of Internet SSO is significant. Consider the following quantifications, were are based on 1,000 users:

- Recovered user productivity from eliminated application logins: \$38,125
- Decreased help desk costs from eliminated password resets: \$21,000
- Recovered user productivity from eliminated password resets: \$6,100
- **Total annual business benefit: \$65,225 per 1,000 users**

As you can see, Internet Single Sign-On alone provides substantial, quantifiable business benefits—enough to easily cost justify Internet Single Sign-On solely based on these metrics. Before incorporating these figures into a formal ROI analysis, there are even more benefits to consider.

3. The Business Value of Internet User Account Management

In addition to the business value from Internet SSO outlined in the previous section, Internet Identity Security software provides business benefit through the automation of Internet user account management. The problem is a simple one: virtually every Internet application requires its own user directory which must be maintained and kept up-to-date. When users leave the organization, for example, access to the application must be quickly removed to prevent unauthorized access and potential data loss.

The Internet User Account Management Dilemma

When Internet applications are first deployed in an organization, account management is often performed manually or as a one-time data load for initial account creation. As the adoption rate of Internet applications increases, however, this can become a management nightmare. Consider one Ping Identity customer who reports 50,000 users accessing four outsourced Internet applications. This is potentially 200,000 separate user accounts that must be managed. The same company predicts that they will increase the number of supported applications to twelve by the end of 2009—increasing the number of potential user accounts to 600,000!

Compliance Issues Solved

In addition to administrative overhead and potential security risks, numerous regulations such as Sarbanes-Oxley, Gramm-Leach-Bliley and HIPAA specify that user account access and password management policies must be in compliance with the law. Some people in IT have a rude awakening when they realize that these regulations apply to both internal and external applications.

One Ping Identity customer, for example, recently failed SOX audits because they could not prove that they were in compliance with SOX requirements for their SaaS applications. Deploying Internet Identity Security software satisfied the auditors' requirements within a few weeks of purchasing the software.

Automation is Key

Ping Identity's products automate the Internet user account management process. PingFederate and PingConnect can automatically create and maintain remote user accounts. For example, Salesforce CRM users are added

to a “group” or “filter” in the organization’s local directory, and PingFederate or PingConnect automatically detect the change and replicate it in the remote Salesforce directory. If a user role is changed, or the user is removed from the group, PingFederate and PingConnect automatically reflect those changes as well.

To summarize, there are three primary business values derived from Internet User Account Management, and each will be discussed in detail below:

- Decreased administrative overhead
- Reduced risk of data theft and unauthorized application access
- Increased compliance audit pass rates

3.1 Business Benefit #1: Decreased Administrative Overhead

Administrative overhead can be a significant downside of outsourced applications. As discussed previously, user accounts are usually required for every outsourced application, and if implemented manually, high administrative costs result. Consider the following:

- Number of Internet application users: 1,000
- Number of Internet applications: 1
- Total number of Internet user accounts: 1,000 (users * apps)
- Average fully burdened labor rate for administrative personnel: \$0.61 per minute¹²
- Estimated Internet user account changes per month: 10% (100 accounts)
- Average time to create or modify an Internet user account: 2 minutes
- Time per year to administer Internet user accounts: 2,400 minutes (100 changes/month * 2 minutes * 12 months)
- **Cost per year to administer accounts: \$1,464 (2,400 * \$0.61), per application, per 1,000 users**

To put this into perspective, 2,400 minutes per year of administrative time is 40 hours per application, per 1,000 users, per year. While this may not seem like a lot, consider that many organizations have many more applications and users than this example illustrates. As the quantity of applications and user counts increase, savings from automating this process rapidly increase.

3.2 Business Benefit #2: Reduced Risk of Data Theft and Unauthorized Account Access

There are two valuable side effects that result from combining Internet SSO and Internet User Account Management. First, since Internet SSO eliminates passwords, it becomes impossible to access Internet applications without first signing on to the organization’s security system (most application providers support this policy). When an employee leaves the organization, application access is implicitly removed when their access is removed in the organization’s directory. Secondly, even if there is an alternate application access method, automating the Internet User Account Management process ensures that

¹² See section 2.1 above for labor rate calculation

remote user accounts are automatically removed or disabled when an employee leaves the organization. Think of it as double insurance against unauthorized access and data loss.

While these are substantial business benefits, they are difficult to quantify. Unless there is a way to assign a value to potential data loss, reduced risk is more of a “soft” benefit. Unless there is a loss, it is difficult to quantify the potential damage. Fortunately most executives innately understand that the risk from Zombie accounts is a significant exposure.

3.3 Business Benefit #3: Increased Compliance Audit Pass Rate

Regulatory compliance has emerged as a key IT and business issue over the past few years. A number of highly publicized compliance violations resulting in fines and even jail time for those convicted of violating the law have resulted in businesses spending a lot more time and money on compliance and risk management.

While most people are not in direct danger of being jailed or fined, high scrutiny on how IT policies and practices align with corporate compliance initiatives is prudent. Most regulations have stipulations around the management of passwords and application access, and regulations generally require proof of compliance along with metrics to back them up, such as auditable logs and reports and fully documented processes.

Ping Identity products can aid in compliance in two different ways. First, Internet SSO provides a convenient, secure, central location for managing and auditing user access to Internet applications. Second, since no passwords are utilized, Internet SSO removes any password-related issues from compliance policies. Third, because Internet user accounts are automatically managed, when employees leave the company there is an automated, fully auditable mechanism in place that allows IT to prove that application access policies comply with regulations.

Quantifying the business value of regulatory compliance can be difficult. One can use potential fines, which can run into the millions of dollars, as one way to justify expenditures that ensure compliance, but even those are difficult to prove unless there has been a past violation or an industry peer that experienced a violation. Consider compliance another “soft” business benefit—substantial value, but difficult to monetize. There are also potential cost savings around decreasing the amount of manual work that is required to complete compliance audits, but at present data is insufficient to fully quantify.

4. The Business Value of Identity-Enabled Web Services

Identity-Enabled Web Services are a next generation Internet application architecture that allows one Internet application to call on another to perform specific tasks, regardless of where they may be located. Due to the nature of the Internet, these requests must be fully secure and Internet-friendly.

There are a number of standards that have emerged to support these interactions, including SOAP (Simple Object Access Protocol) and REST (Representational State Transfer). One aspect of Web Services that has been lacking standards until the past few years was security—in order to provide fully secure and personalized user experience, the identity of the initiating

user must be securely passed between Web Services. Identity-Enabled Web Services leverage these new standards, allowing Web Services to securely share user identity regardless of their location.

In terms of business value, Identity-Enabled Web Services are generally considered “soft” benefits, as increasing the security of Web Services applications by passing identity is significant, yet difficult to quantify. Most organizations consider this a business enabler, as Web Services reduce business friction and increase user experience by providing end-to-end Web Services security and personalization.

Take, for example, a major online retailer that decides to implement a rewards program for its loyal customers. The retailer contracts with a service provider to provide tracking and reporting for its loyalty program. The service provider implements the loyalty program as a series of Web Services that must be called from the initiating retailer’s Web server, and the customer’s identity must be passed along to the service providers’ Web Services in order to provide a seamless, fully personalized experience. By leveraging the WS-Security standard, the retailer is able to securely pass its user’s identities across to the service provider.

To summarize, the business benefits of Identity-Enabled Web Services are as follows:

- Identity-Enabled Web Services easily interface with one another using a secure, standards-based mechanism that requires minimal custom coding and integration, reducing deployment costs
- Applications that use Web Services are more personalized, resulting in improved user experience

5. Internet Identity Security ROI

This section is intended to provide a brief overview of how to calculate Return on Investment (ROI) of an Internet Identity Security investment.

Before we delve into the details of the business value of Internet SSO, a few business case terms should be defined:

5.1 Return on Investment (ROI)

ROI is the gold standard for measuring business value from an investment. Generally expressed as a percentage value over a fixed time period (one and three years is common), ROI provides an easy-to-understand measure of the overall performance of a given investment over time.

The ROI formula used by Ping Identity is based on one created by the United States Financial Standards Account Board (FASB), commonly known as the Generally Accepted Accounting Principles (GAAP) standard.

The GAAP formula for calculating ROI is as follows:

$$ROI = \frac{(Gain\ from\ Investment - Cost\ of\ Investment)}{Cost\ of\ Investment}$$

In other words, ROI expresses the net benefit derived from an investment, divided by the cost. This is expressed as a percentage, generally calculated

over a three year period since many investments do not pay for themselves in a short period of time. The following formula takes into account three years of benefits and costs:

$$ROI = \frac{(Year\ 1\ Benefit + Year\ 2\ Benefit + Year\ 3\ Benefit) - (Year\ 1\ Cost + Year\ 2\ Cost + Year\ 3\ Cost)}{Year\ 1\ Cost + Year\ 2\ Cost + Year\ 3\ Cost}$$

Note that ROI is generally multiplied by 100 in order to get a 'real' percentage (e.g. 200%).

5.2 Net Present Value (NPV)

ROI formulas such as the one outlined above are commonly used by technology vendors to help sell their products, as a basic ROI can yield very impressive results as it does not take other factors, such as potential alternative investments, into account. Net Present Value, or NPV, reduces the potential ROI by accounting for an alternate use of the money, such as investing it in a bank account.

NPV expresses the value of a dollar today to the value of the same dollar in the future, taking inflation and returns into account. In other words, NPV calculates the net benefit of a project using today's dollar terms, assuming that the value of a dollar will fall in the future due to inflation and other factors. The "net" part of NPV is the difference between all of the costs and all of the benefits, including savings and other gains. The "present value" component takes into account the time value of money, adjusting expenditures and returns as they occur over time so that they can be evaluated equally.

A real-world example of NPV would be as follows. Assume that you are considering investing \$100,000 into a certain technology. If you take the net benefits that are expected to be received from that investment over time (say three years), and then discount them into one lump sum, you have the NPV. If the NPV is greater than \$100K, then the investment is sound, and the greater the NPV, the better the investment.

The NPV formula is:

$$NPV = \frac{R_t}{(1 + r)^t}$$

In English, NPV for any particular year 't' equals "Rt" (the net benefit (benefit minus cost) per time period (generally a year)), divided by (1+r), where 'r' is the cost of capital, otherwise known as the Discount Rate. A Discount Rate of 5% is a commonly accepted value, similar to the rate of inflation. It is also possible to specify a higher Discount Rate if a specific capital cost is known, such as an alternate investment. If NPV is less than zero, then the investment is a poor one, as it loses money compared with the discount rate. An NPV of zero reflects a break-even investment, and a positive NPV reflects a positive profit from the investment.

5.3 Time-to-Value (TTV) and Payback Period

Time-to-Value, or TTV, is a simple yet very important concept: how long does it take before a given investment begins delivering substantial value to the organization? This is a function of implementation and deployment time, and the faster the TTV, the shorter the payback period.

Payback period is another simple concept. How long does it take before a given investment is paid back in full? In other words, how long does it take to reach a 100% ROI? That is generally regarded as the “break-even” period for an investment.

5.4 Total Cost of Ownership (TCO)

Total Cost of Ownership, or TCO, is another extremely important metric. When calculating an ROI, the total cost of the investment must be considered. Oftentimes, technology purchases are scrutinized on the amount of initial outlay (software license plus maintenance), but there are many other costs that need to be considered, such as:

- Training and implementation services
- Additional hardware and software required for scalability
- Ongoing administrative costs
- Deployment and rollout expenses

Investments with the lowest TCO have a short TTV and payback period, and achieve maximum ROI more quickly. Many vendors in the Internet Identity Security space have a low up-front purchase cost, but a high TCO due to extensive customization services and high ongoing maintenance. Ping Identity’s products have very low TCO compared to other alternatives in the market.

5.5 An Example PingFederate Internet Identity Security ROI Calculation

The following ROI calculation represents a typical Internet Identity Security deployment and is based on a 1,000 user deployment using Ping Identity’s PingConnect hosted Internet Identity Service to access a SaaS application such as Salesforce CRM or Google Apps.

5.5.1 Total Cost of Ownership

When calculating costs, it is important to break them down into a three year period so that the business benefits can be amortized on a year-by-year basis. This affects the TTV, TTP and ROI values for each year. For PingConnect, cost calculations are simple due to a simple “on demand” pricing scheme of \$1 per user per month per application. Costs of the PingConnect deployment with 1,000 users and one SaaS application are broken down as follows:

- PingConnect Subscription Cost: \$1,000 per month; \$12,000 per year
- Year 1 implementation and administrative cost: \$5,000 (estimated: includes set up fees and customer configuration time)
- Years 2 and 3 implementation and administrative cost: \$1,000 (estimated)
- TCO, year 1: \$17,000
- TCO, year 2: \$13,000
- TCO, year 3: \$13,000

5.5.2 Business Benefit Calculations

To keep the ROI calculation simple and straightforward, we will only consider “hard”, fully quantifiable business benefits in the calculation, as follows:

- Increased Employee Productivity: \$38,125¹³ per 1,000 users
 - 3 app logins/day, 1 application, 5 second login time
- Decreased Help Desk Costs: \$21,000¹⁴
- Increased user productivity from reduced help desk calls: \$6,100¹⁵
- Decreased Administrative Overhead: \$1,464¹⁶
- **Total Benefit, per Year, per 1,000 users: \$66,689**

5.5.3 Internet Identity Security ROI and Payback Calculations

Using the simple ROI formula outlined above, the ROI calculation is as follows:

$$ROI = \frac{(Benefit - Cost)}{Cost}$$

$$First\ Year\ ROI = \frac{66,689 - 17,000}{17,000} = 292\%$$

$$3\ Year\ ROI = \frac{(66,689 + 66,689 + 66,689) - (17,000 + 13,000 + 13,000)}{17,000 + 13,000 + 13,000} = 365\%$$

This is a substantial return on investment. It is clear, just from “eye balling” the formula, that the investment reaches 100% ROI very quickly after deployment. If you divide the annual business benefit of \$172,190 by 12 to reach a monthly figure of \$14,349, and divide the total three year cost of \$77,000 by the monthly benefit, 100% payback for the entire project is reached somewhere during the fifth month of deployment.

Next, the net benefit over a three year period is computed in order to determine the payback period:

- Year 1 Net Benefit: \$49,689 (\$4,141 per month)
- Years 2,3 Net Benefit: \$53,689 (\$4,474 per month)
- Average Net Benefit (over 3 years): \$4,363

Using the net benefit calculations, computing time-to-payback is straightforward:

- Year 1 cost / Year 1 monthly benefit = \$17,000 / \$4,141 = 4 month payback
- Total year 1 to 3 cost / average monthly benefit = \$43,000 / \$4,363 = ~10 month payback for entire 3 year project

13 See section 2.1 above for full details on this calculation

14 See section 2.2 above for full details on this calculation

15 See section 2.2 above for full details on this calculation

16 See section 3.1 above for full details on this calculation



Conclusions from ROI and Payback Calculations

Based on the calculations presented above, a 1,000 user PingConnect implementation for just one SaaS application will achieve a 292% first-year ROI and will payback the investment in just 4 months. Over a three year period, PingConnect will deliver a 365% ROI and the entire project will achieve payback in just 10 months. Keep in mind that this is just for one SaaS application—adding additional applications and users drastically increases the benefit as economies of scale take effect.

5.5.4 Calculating Net Present Value and Risk-Adjusted ROI

As outlined above, the NPV calculation for the three year investment is as follows. Note that an 8% Discount Rate was chosen instead of the standard 5% value in order to compare this investment with an alternate investment yielding an 8% return.

- NPV, year 1: $(\$66,689 - \$17,000) / (1 + 8\%)^1 = \$46,008$ (\$3,834 monthly)
- NPV, year 2: $(\$66,689 - \$13,000) / (1 + 8\%)^2 = \$46,030$ (\$3,836 monthly)
- NPV, year 3: $(\$66,689 - \$13,000) / (1 + 8\%)^3 = \$42,620$ (\$3,552 monthly)
- Total NPV, Years 1 to 3: \$134,658 (average monthly benefit: \$3,741)
- NPV-based ROI, Years 1 to 3: $\$134,658 / \$43,000 = 313\%$
- Time to payback, year 1: $\$17,000 / \$3,834 = \sim 5$ months
- Time to payback, 3 years: $\$43,000 / \$3,741 = \sim 12$ months

Conclusions from NPV-based ROI and Payback Calculations

Based on computations above, which compared the three year PingConnect benefit against an 8% potential investment, yielded a **313% ROI over three years and 100% payback for the entire three year project in twelve months.**



Figure 1: Comparing returns of a standard 8% investment with Internet Identity Security



6 Conclusion

This paper demonstrated a number of key business values delivered by Ping Identity's Internet Identity Security products, PingFederate and PingConnect. Benefits may be classified in terms of "hard", easily quantified values, and "soft", intuitive but hard to quantify values. A summary of the hard business benefits and quantifications discussed in this paper follows. Note that these are all the same calculations found above.

Benefit Area	Example Quantification
Decreased help desk costs due to reduction in password-related Calls	\$21,000 per year, based on only one help desk call per year per employee, and a total of 1,000 users
Increased employee productivity from reduced help desk calls	\$6,100 per year per 1,000 users, based on commonly accepted labor rates
Increased employee productivity from Internet SSO	\$38,125 per year, per application, per 1,000 users, based on commonly accepted labor costs
Increased revenue due to increased employee productivity	Varies; a highly profitable pharmaceutical company, for example, could be as much as \$311,250 per year.
Decreased administrative costs due to automated Internet User Account Management	\$1,464 per year per Internet application, per 1,000 users
Total business benefits	From \$66K to \$378K per year per 1,000 users (benefits scale higher as additional Internet applications and users are enabled)

Table 1: Summary of Internet Identity Security Hard Benefit Quantifications

You can also factor in soft benefits to add to the business case:

Benefit Area	Potential Quantification
Increased Internet application adoption rate	Calculate the "critical mass" adoption point required to achieve payback from the application; Calculate the business benefit derived from the Internet application and use the ConAgra example described above to model the value from increased adoption rate



Benefit Area	Potential Quantification
Reduced risk of data theft and unauthorized application access	Calculate the cost of downtime during recovery of critical Internet application data
Increased compliance audit pass rates	Calculate savings from reduced audit costs and avoidance of fines for non-compliance
Identity-Enabled Web Services interface with other Web Services using secure, standards-based mechanism	Calculate cost savings from leveraging standards-based interface; compare against with development time for custom interfaces
Applications that use Web Services are more personalized, resulting in improved user experience	Calculate potential revenue increase due to improved user experience and potential increased competitive ability

Table 2: Summary of Internet Identity Security Soft Benefits

If you incorporate even a few of the benefits of Internet Identity Security software into a well reasoned business case that illustrates just how much value the organization will receive from the investment, there is a high probability that the project will be approved.

After deploying PingFederate or PingConnect, which is a highly visible win for IT and the business, the organization will run more efficiently and will have a distinct competitive advantage over companies that do not leverage Internet Identity Security Software. See for yourself by going to www.pingidentity.com or calling +1.303.468.2882 today.

About Ping Identity Corporation

Ping Identity is the market leader in Internet Identity Security, delivering on-premise software and on-demand services to more than 300 customers worldwide. For more information, dial U.S. toll-free 877.898.2905 or +1.303.468.2882, email sales@pingidentity.com or visit www.pingidentity.com.

© 2009 Ping Identity Corporation. All rights reserved. Ping Identity, PingFederate, PingConnect, PingEnable, the Ping Identity logo, SignOn.com, Auto-Connect and Single Sign-On Summit are registered trademarks, trademarks or servicemarks of Ping Identity Corporation. All other product and service names mentioned are the trademarks of their respective companies.

