Essential Steps for Implementing Strong Authentication in the Enterprise

Symantec

Table of Contents

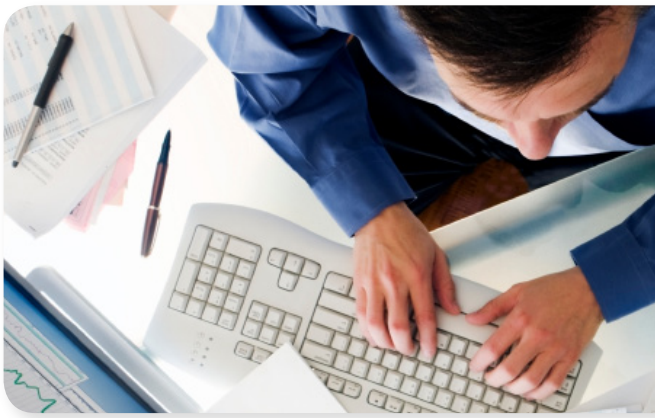
Symantec

Executive Summary

Corporations are increasingly extending access and exposing information to corporate data in order to run their businesses more effectively. In the process, however, one could say that they are locking the doors but opening windows when it comes to securing information. While they are clearly "locking the doors" to the network with security safeguards such as firewalls, email and web filtering technologies, they are also opening up "windows of access" to a vast array of corporate information through the use of technologies like mobile computing, data sharing, SaaS and Web 2.0 applications, among others.

Corporations cite clear business cases as to why they're rapidly opening up their environments, not the least of which are streamlined processes, increased agility and greater efficiencies. But they must find a solution to deal effectively with the risks associated with a more open environment—a solution that also meets corresponding partner obligations and regulatory requirements. According to Forrester, few are doing so. In fact, most organizations still use simple user name and password as the only for of authenticating employees and partners into their network. Despite the solution's well-documented successes, only 30% are adequately securing their information through the use of strong authentication technologies.

It therefore comes as no surprise that security breaches have increased rapidly in the last 12 months. According to Forrester, 54% of all enterprises suffered a breach in the last year, while a third of those surveyed suffered three or more.



54% of all enterprises suffered a breach last year

Companies must immediately begin to look at access to information — whether that information is accessed by mobile employees, partners or customers — as a critical component to a comprehensive security strategy. Two-Factor Authentication has matured — the cost of the technology has dropped significantly, while the evolution of cloud-based solutions has made technical complexity a non-issue. No longer is it necessary for employees to carry cumbersome tokens and also remember passwords — now, the simple (and ubiquitous) cell phone is all that's required to offer enterprise protection from hackers, phishing attacks, Man-in-Browser attacks and other forms of unauthorized access.

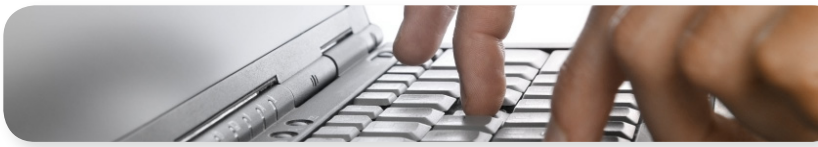
Symantec

Introduction

For decades now corporations have been in a battle to protect the business while at the same time striving to improve business processes and make information readily and easily available to employees, customers, partners, and other stakeholders. A delicate and often times precarious balance has been the result which, even when temporarily achieved, is regularly thrown off kilter with the rapid adoption and evolution of new technologies. Applications are now Internet-enabled and allowing employee access to the intra- and extranets through mobile devices has become an essential component of doing business. Compounding that, business partners are often provided entry to ensure everything from immediate access to information to the attainment of service level agreements.

The downside of all this has been the rapid erosion of the once relatively secure perimeter. Companies must now ensure the integrity of their data against all of the threats of the last generation (viruses, etc.) as well as all of the modern-day threats associated with having information available to various parties all over the world at all times, and with an unprecedented number of venues through which one may gain access to that information.

An August 2010 study conducted by Forrester Consulting and commissioned on behalf of VeriSign (now Symantec) entitled "Enhancing Authentication to Secure the Enterprise," provides a thoughtprovoking examination into how companies today are dealing with 21st century threats such as phishing, hacking and unauthorized access, while simultaneously streamlining business processes through the use of new and evolving trends and technologies such as remote access capabilities, third-party access, Web 2.0 technologies and Software-as-a-Service applications.



> "...while enterprises are aware of the threats and consider them very real, they have not taken sufficient action to protect themselves"
>
> "Enhancing Authentication to Secure the Enterprise"
> — Forrester Consulting, August 2010

In short, the study clearly indicates that while enterprises are aware of the threats and consider them very real, they have not taken sufficient action to protect themselves.

In the following document, we'll further explore the situation and make five recommendations as to how corporations can better secure their environments while also reaping the benefits that new technologies such as Web 2.0 and mobile access bring to the table. Finally, we'll provide a brief overview of Symantec's strong authentication technology offerings.

Symantec

Strong Authentication Defined

Basic authentication is the process by which a computer system positively identifies a user, and is generally required to access secure data or enter a secure network. The dominant authenticationsystem in use today is based on user names and passwords, commonly considered to be one of the weakest security links in modern day computing.

This system is subject to a number of flaws, including poor user password choices, password harvesting, phishing and man-in-browser attacks, among others.

> A Two-Factor Authentication system works by requiring two simultaneous but independent authentication methods commonly referred to as "something you have and something you know."

The most common and compelling solution to authentication problems is the use of Strong Authentication, otherwise referred to as Two-Factor Authentication. A Two-Factor Authentication system works by requiring two simultaneous but independent authentication methods commonly referred to as "something you have and something you know." Normally, the first factor (something you have) involves hardware or software that provides the user with an electronically generated passcode or digital certificate that serves as a unique identifier for a particular user which is then coupled with the second factor (something you know) such as a password that together constitute a strong authentication system for enabling access to critical resources like a corporate network. Two-Factor Authentication systems are made secure because it is very difficult for non-legitimate users to obtain both of these factors.

According to experts, Two-Factor Authentication dramatically reduces the incidence of online identity theft, phishing attacks, and other online fraud, because the victim's password is simply no longer sufficient to give a thief access to their information. Following are five key recommendations for implementing Two-Factor Authentication in the enterprise.

Symantec

Recommendation #1

Understand the true nature of today's IT usage within your corporate environment.

It is imperative that organizations understand exactly what technologies are being used inside and outside the organization to access information, and how that usage maps to the current IT policies and protections that are in place.

All too often, corporate security policies have not kept up with the rapid changes that have occurred over the last few years. Forrester research data has identified a number of technologies and trends that have been widely adopted throughout the enterprise without sufficient thought to the possible repercussions of implementing or allowing these technologies to proliferate.

60% of enterprises today are using at least two SaaS Applications

Following are some examples:

Personal computers and devices

Employees are today more mobile than ever before, and companies are not only allowing but even encouraging employees to access corporate information through devices such as personal computers and smart phones. In the process, companies are again opening up their environments to devices over which they have no direct control.

Software-as-a-Service applications

There's no question that SaaS offers an enormous range of benefits. In fact, nearly 60% of enterprises today are using at least two SaaS applications. One out of five is using 6 cloud-based applications or more. And the numbers are expected to increase rapidly. SaaS solves many problems for an IT manager, but at the same time introduces a number of potential pitfalls. Namely, many SaaS providers have adopted weak authentication mechanisms—simple passwords for access to vital information. And as we've seen proven again and again, passwords have long ceased being adequate protection for valuable data. How can businesses continue to justify and allow the movement of sensitive information to the cloud if that information can be accessed by a simple password?

1 out 5 is using six cloud-based applications or more

Symantec

With the possible exception of online banking, that is precisely what's happening today. SaaS providers must support strong security measures to protect the data of their clients. As a rule of thumb, it's a good idea to select SaaS vendors that protect their customers with strong authentication no matter what kind of information they're dealing with. It never hurts to lock up information whether it's considered confidential or not—no one ever got in trouble for locking a safe.

However, if you are sharing information with your SaaS vendor that involves personally identifiable information such as in Human Resource applications, two-factor protection is required. In addition, any information such as financial statements, sales pipeline, board reports, customer information, budget reports, partner information and many other forms of data make the use of two-factor protection essential. With all this, it is easy to see why the easiest mandate would be for a company to require Two-Factor Authentication across all of its SaaS providers, regardless of the type of information shared.

We can look at the relationship between strong authentication and SaaS applications in another way as well by considering the companies that are not employing SaaS applications due to concerns over security measures.

When asked why their firms were not interested in Software-as-a-Service, the largest response—nearly half of all those surveyed--responded "security concerns." (Global IT Budgets, Priorities, And Emerging Technology Tracking Survey, Q2 2010) Forrester reports that 45% of those not adopting SaaS applications cited security as a main reason for not doing so, which begs the question: What are these businesses losing out on in terms of increased productivity, increased sales and improved business processes by eschewing the technology over security concerns? It would be advisable for companies to consider a cost-effective solution that would solve their security concerns and thereby allow them to take advantage of the many benefits and wide variety of SaaS solutions.

45% of (firms) not adopting SaaS applications cited security as a main reason for not doing so

Web 2.0 Applications

In early 2010, Forrester Consulting surveyed corporations in order to learn their greatest concerns in terms of new technologies and initiatives. Not surprisingly, the largest concerns revolved around the increasing use of Web 2.0 technologies and the use of smart phones in business. [January 25, 2010 The State Of Enterprise IT Security And Emerging Trends: 2009 To 2010 by Jonathan Penn for Vendor Strategy Professionals]

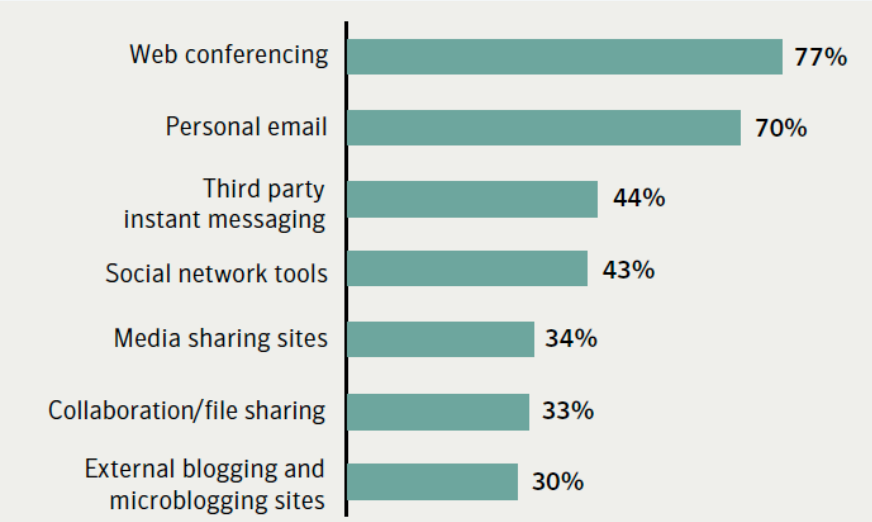
Symantec

According to the report, this kind of "consumerization" in the workplace ranks highest among concerns because it "represents a greater loss of control of oversight in the computing infrastructure." The study found conclusively that business and personal environments have merged. That merger has opened up a number of new technologies into the corporate environment and though businesses feel they've benefitted from them, they are also clearly aware of the added security risk these technologies bring, and are concerned largely because they have not yet fully acted to mitigate them.

Additionally, the growing prominence of extranets, cross-organizational collaboration tools, and Web 2.0 applications, mean non-employees such as customers, suppliers, and business partners increasingly gain access to corporate applications and data, oftentimes through new social media technologies. Extending the network can help organizations cut operational costs through greater process efficiencies, promote crossorganizational innovation and eliminate the need to build costly and time-consuming point-to-point connections. Although there are tremendous benefits to this expansion of the corporate network, the need for strong security has never been more apparent.

More Business Communication Is Taking Place Outside Of Corporate Systems

What external communication and collaboration technologies do your users have access to?



Source: A commissioned study conducted by Forrester Consulting on behalf of VeriSign, August 2010

Symantec

Authentication and password policies

In general, companies have responded to an increasing number of security threats by using outdated technologies, made "stronger." Today, an employee continues to gain access to company information through the use of a password.

85% of companies surveyed require users to "remember" at least 2 passwords

What's changed is that the password must now be eight or more digits long, must include symbols and numbers and must be changed as often as every few months or more. In addition, the employee may need different passwords to access different areas of information--different databases, different areas of internal networks, etc. The flaw in requiring employees to memorize new serial-number-length passwords containing symbols, numbers and letters every few months is obvious. And the common result is that passwords are simply written on sticky notes and stuck to a laptop. Not the fool-proof and secure implementation the IT department had in mind.

66% of companies have at least six different password policies

To illustrate the point, Forrester found that 85% of companies surveyed require users to "remember" at least 2 passwords. 66% of companies have at least six different password policies. The result has been that 80% of companies considered password issues—and specifically the challenge users have in managing multiple passwords with complex policies on construction and expiration- -to be the single biggest complaint about information access. And how do companies continue to respond to actual data breaches? Nearly two-thirds were found to have implemented more manual procedures and controls!

80% of companies considered password issues to be the single biggest complaint about information access

Many corporations are simply defaulting to more and more obtuse password policies because it's seen as the least expensive solution to the problem. But the increased help desk calls that result from password issues invariably result in higher demands on IT resources.

According to another Forrester report, "Password problems and resets generally constitute between 25% and 40% of total help desk incidents." [Twenty-three Best Practices for the Customer Service Center, Chip Gliedman, October 11, 2005]

Gartner Group estimates that between 20% and 50% of all help desk calls go into the Password Assistance Bin. In one eye-opening Gartner Group case study, a global beverage company found that 30% of their help desk calls were password related, and each call carried with it a $17.23 price tag. This resulted in an annual cost to the company of $900,000. Forrester Research goes a step further to estimate that when we in-

Symantec

clude the average help desk labor cost for a single password reset the total jumps to about $70 per call. Needless to say, “stronger” passwords are not the inexpensive answer some think they are.

Third-Party Access

Third-party access to information has become common among enterprises and deservedly so. As with the implementation of SaaS applications, companies can enjoy immediate and significant improvements to their businesses. But when it comes to allowing network access to a partner, there is one very important rule to remember: When you grant access to a third party, you automatically reduce your level of security to their level of security. If they have insufficient security controls, then they bestow upon you those very same insufficient security controls. If and when their systems are compromised, a hacker may well find himself a window into your network.

And what is the potential cost to the business? Unknown. But just consider the effect on a care-fullynurtured reputation. If and when malicious access to your network is achieved, even if that access comes through a trusted partner, your company will still be held accountable, and your customers will care about the origination of the breach. Needless to say, negative media coverage about a security breach can have a devastating and long-term impact on business.

It is also important to understand that granting external access to partners, often means relaxing firewalls restrictions and other controls. In short, a company that allows easy access to partners into their network is creating a huge window of opportunity, waiting to be exploited.

There are without a doubt as many reasons to grant access to trusted partners as there are companies in existence today. However, these partners should be treated with at least the same level of scrutiny and care as would be a mobile employee of the company. And extending Two-Factor Authentication to partners is a great way to offer another layer of protection to the network.

When you grant access to a third party, you automatically reduce your security to their level.

Symantec

Recommendation #2

Ensure strong authentication for all employees and partners coming into your organization

Not only are sales people accessing critical information from outside, but so are field marketing, home based employees, partners, and many others.

For all the reasons listed above, corporations should expand Two-Factor Authentication to a state of complete coverage across the organization. Not only are sales people accessing critical information from outside, but so are field marketing, home based employees, partners, and many others. Furthermore, employees may soon (if they're not already) be accessing Internet applications from within the network.

Regardless of the threats, Forrester recently found that less than 1/3 of all the companies surveyed used Two-Factor Authentication as the primary method of authenticating legitimate users into the corporate network.

43% of the companies surveyed currently use strong authentication technology for VPN access only, and more than 25% use no form of Strong Authentication whatsoever.

Furthermore, up to 75% of companies allowing partner access to resources do not utilize a second factor for authentication. This is due to an alarming misconception. While a paltry 20% of companies express concern about breaches resulting from misuse or abuse by a business partner, security analyst PONEMON has recently found that 42% of all breaches did in fact involve third-party "mistakes," and the result of those breaches were actually more expensive for the companies that suffered them than were breaches of other origination. This points to an obvious chasm between the comfort level companies have with partners accessing data and the level of comfort they should have based on reality.

75% of companies allowing partner access to resources do not utilize a second factor for authentication

Complete coverage may not be realistic especially in large enterprises. In this case they should adopt a graduated strategy of deployment starting with critical employees and management that have access to the most compromising data. But it should be considered mission-critical that companies ensure all partners are provided with a strong authentication solution as limited knowledge about the level of security deployed in any one partner's organization may leave them

Symantec