



October 2009

The Need for Two-Factor Authentication at Enterprise Organizations

Research conducted by:

InfoWorld

Sponsored by:

 **VeriSign**[®]

Contents

- Overview 3
- Profile of Respondents. 3
- Executive Summary. 6
- Usage of authentication factors. 7
- Effectiveness of authentication systems 9
- Areas for major changes to authentication systems 10
- Important factors when evaluating an authentication solution 11
- Performance of current authentication solutions 11
- Usage of two-factor authentication 12
- Challenges of adopting two-factor authentication 12
- Familiarity with cloud computing. 13
- Potential benefits of cloud computing 13
- Adoption of cloud services for authentication systems. 14
- Experience with cloud computing 14
- Conclusion. 15

The Need for Two-Factor Authentication at Enterprise Organizations

Overview

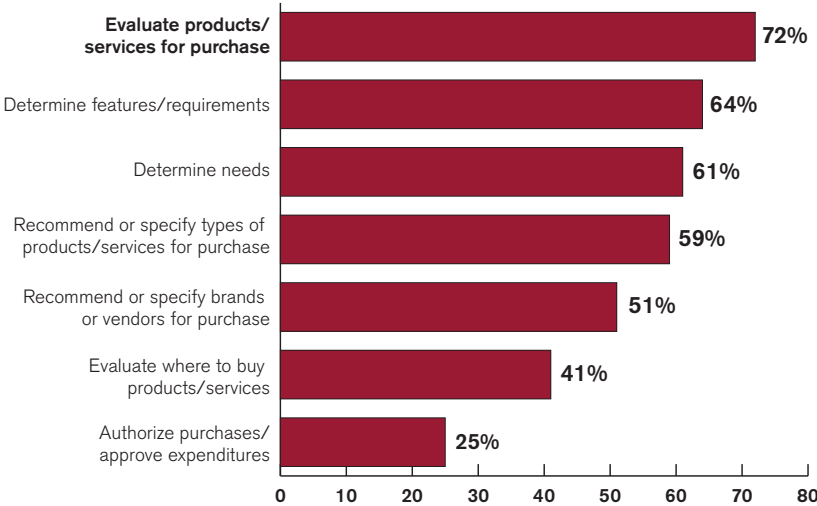
In September 2009, *InfoWorld* invited IT leaders to participate in a survey on authentication solutions. The survey was fielded via targeted broadcasts to *InfoWorld* customers, as well as through an invitation on InfoWorld.com. The goal of the survey was to determine usage of two-factor and cloud-based authentication at medium-size and large organizations. The survey was commissioned by VeriSign, but the data was gathered and tabulated independently by InfoWorld Research. The following report represents top-line results of that survey.

Profile of Respondents

Total respondents: 155

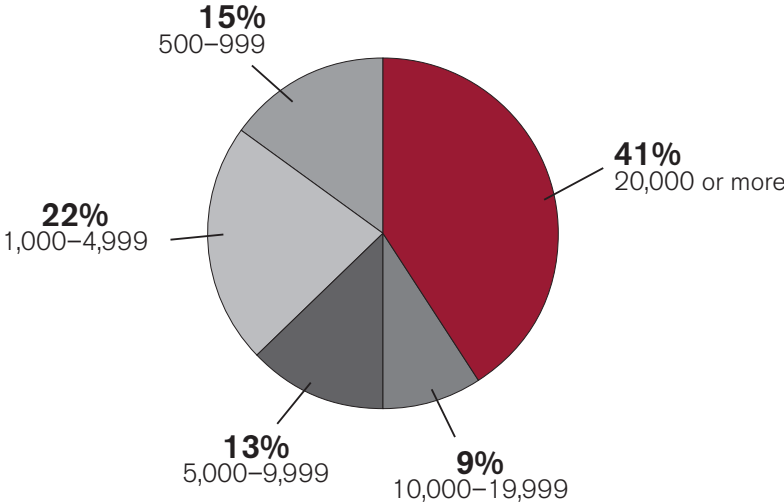
All respondents were qualified through a series of screening questions for involvement in the acquisition of IT security products and services at organizations with 500 or more employees. The chart below provides a breakdown of the percentage of respondents based on involvement. This chart is followed by breakdowns of respondents based on company size, job title and industry.

How are you involved in the acquisition of IT security products and services at your organization?



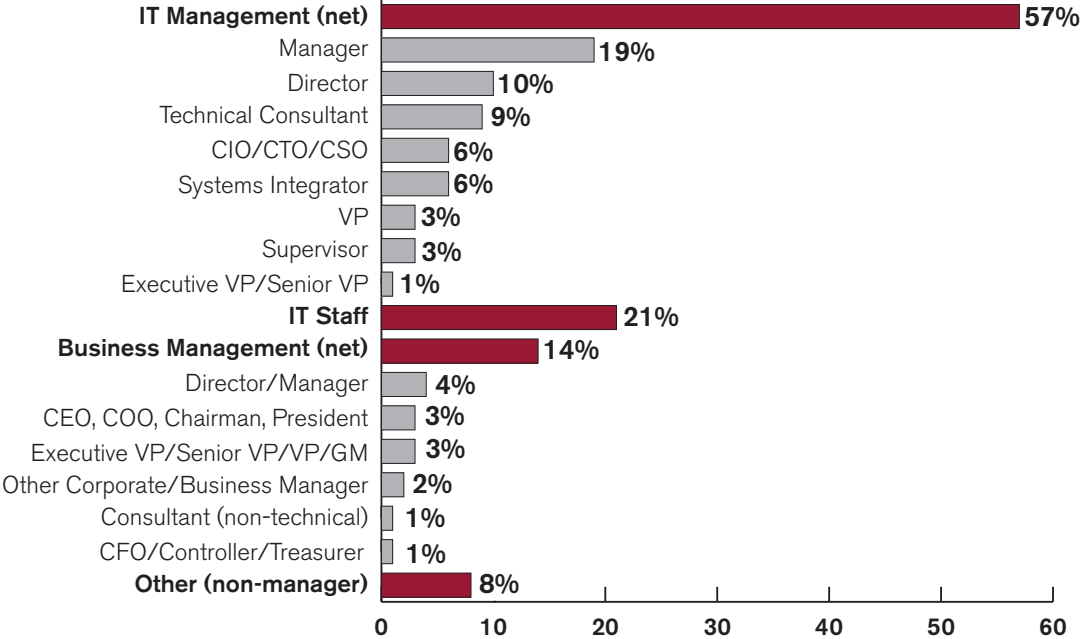
Multiple responses accepted

How many people are employed in your entire organization including all branches, divisions and subsidiaries?

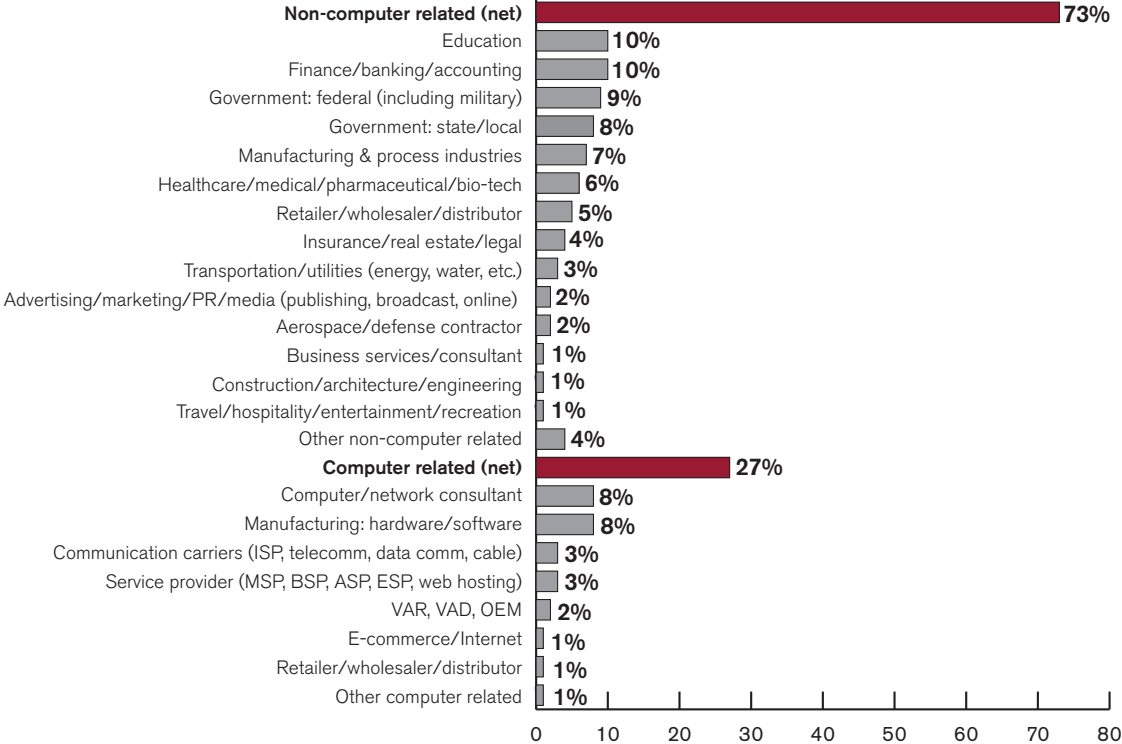


Mean number of employees = 11,350

What is your primary job title?



Which of the following best describes your organization’s industry or function at this location?



Executive Summary

As organizations make the move to digitize their businesses, the need for best practices in the security of technological systems intensifies. Almost all organizations have some type of sensitive information, whether it is personnel records, confidential documents or proprietary company products. That sensitive information needs to be protected from external and/or internal breaches of digital systems. In the age of wireless and remote access, securing this data is becoming more difficult, as wireless and remote capabilities open up a new set of vulnerabilities.

For some time now organizations have been using different types of authentication solutions to ensure that those trying to legitimately gain access to certain information are permitted. Almost all respondents to this research (97%) have used or currently use usernames and passwords to protect their data. While 73% use digital certificates and 54% use PKI certificates or magnetic cards to authenticate their users, respondents most frequently cite biometrics (20%) as an authentication solution they plan to use in the next 12 months or are considering for use in the next 12–24 months.

While more than nine out of 10 respondents rate their companies' authentication systems' effectiveness at addressing compliance and/or industry requirements and protection of their company networks as very or somewhat well (94% and 93%, respectively), areas with more room for improvement include preventing fraud, intrusion or account takeover (86%), desire to boost customer confidence in the security of private/sensitive data (84%), increase in the number of remote/mobile workers at their organization (81%), and especially user/customer demand for simpler methods of accessing information (66%).

This need for change to authentication systems also comes to light as more than one-third of respondents (37%) expect to be making major changes to their authentication systems for desktops/laptops within the next 12 months. Other top areas for major changes within the next 12 months include customer-facing web applications (32%), WAN (29%), databases (28%), business applications (28%), servers (28%) and email (27%).

It is apparent that there is room to improve various areas related to authentication solutions, with the highest rating for current authentication solutions as scalability/flexibility (56% rating excellent or good) and total cost of ownership at 54%. Just under half of all respondents (49%) rate their authentication solutions as excellent or good for the level of IT resources required for maintenance. Paralleling those findings, respondents report the following as critical or very important factors when considering an authentication solution: increased scalability/flexibility (83%), lowered costs (81%) and reduction of burden on IT resources/staff (78%).

As those with the malicious intent to breach organizational security systems become smarter, so must that organization's authentication system. A way to add an additional layer of protection is to invest in a two-factor authentication system, thereby making it more difficult to hack. Currently, just half of all respondents (50%) are using two-factor authentication. An additional 20% of respondents are considering two-factor authentication systems within the next 12 months. Almost one-third of respondents (30%) have no immediate plans to use a two-factor authentication solution.

When implementing any new system there will be challenges and barriers. Roughly two-thirds of respondents (65%) are concerned with the complexity of a two-factor authentication system as well as integration issues they might have with their current systems. Not surprisingly, the expected barriers and challenges of two-factor authentication adoption are closely aligned with what is important when evaluating an authentication solution, including initial investment costs (56%) and pressure on IT resources (56%).

One way to reduce some of these barriers is through the relatively new concept of cloud computing. Because cloud computing uses a third-party service for storage and management, it has the ability to alleviate some of the pressures respondents feel when considering adoption. Almost nine out of 10 respondents (87%) are very or somewhat familiar with cloud computing. The top benefits associated with cloud computing are increased mobility (59%), scalability (57%), flexibility (52%), reduced cost (51%) and the freeing up of internal IT resources (48%).

Only 13% of respondents have used or are currently using cloud services for their authentication systems. While 34% plan to use cloud services for authentication within the next 24 months (10% within the next

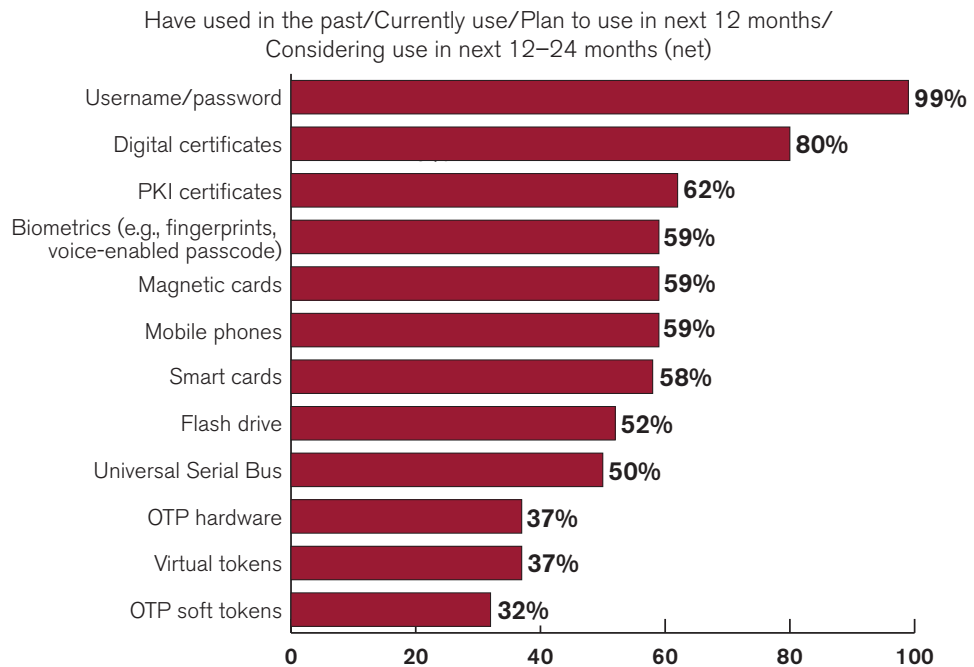
12 months and 24% within the next 12–24 months), more than four out of 10 respondents (41%) have no plans to use cloud services for this purpose.

Among those currently using cloud services for authentication systems or have used them in the past, 85% rate their experience with cloud in regards to increased storage space as excellent or good. Eight out of 10 respondents (80%) also rate their experience as excellent or good for flexibility and scalability. Three-quarters of respondents (75%) have had an excellent or good experience with cloud for increased mobility, while 70% rate an excellent or good experience with easier implementation.

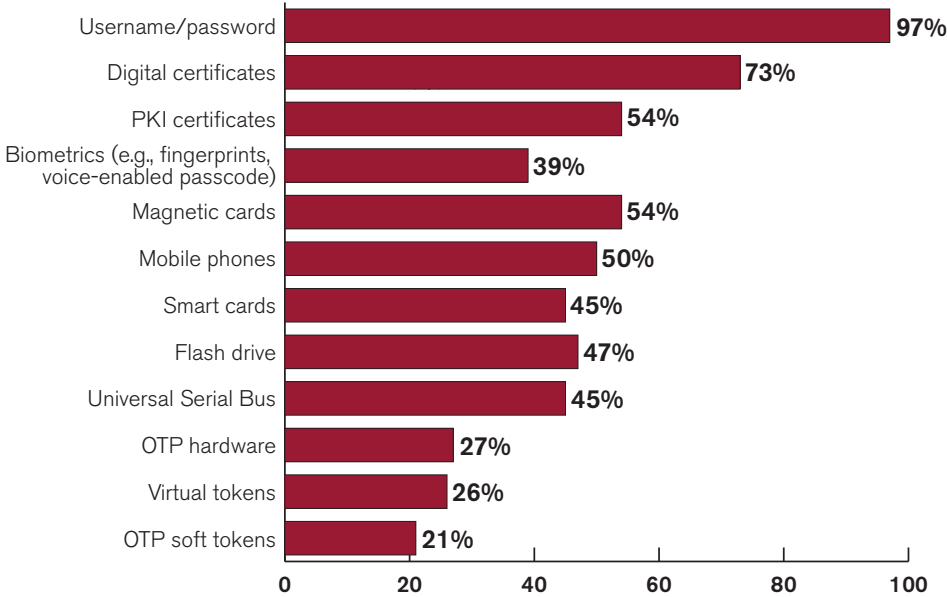
Usage of authentication factors

While virtually all respondents (97%) have used or currently use usernames and passwords for authentication, followed by digital certificates (73%), PKI certificates (54%) and magnetic cards (54%), the top authentication factors planned for use within the next 12 months or being considered for use in the next 12–24 months include: biometrics (20%), smart cards (14%), OTP soft tokens (11%) and virtual tokens (11%).

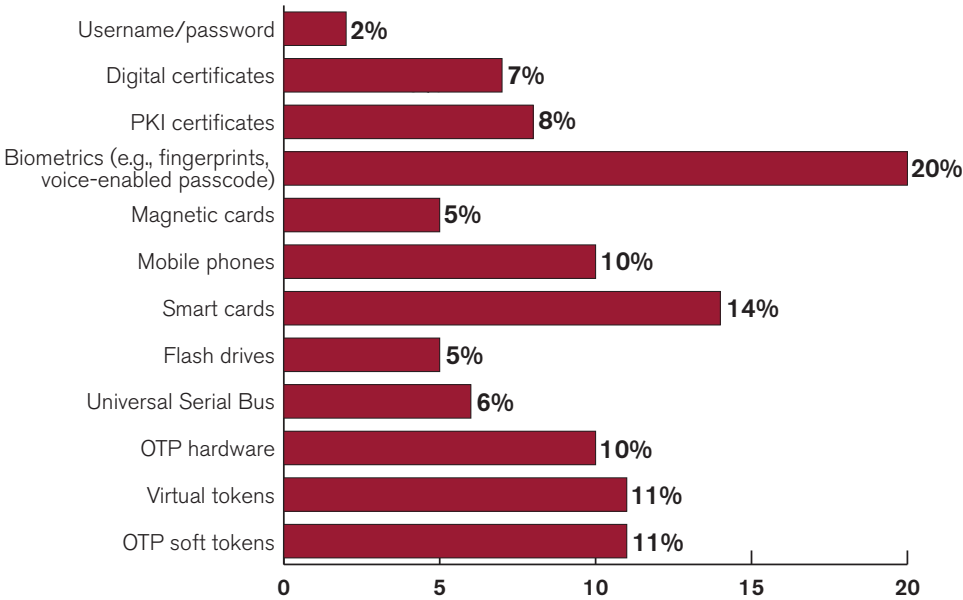
Which of the following best describes your organization’s usage of each type of authentication factor?

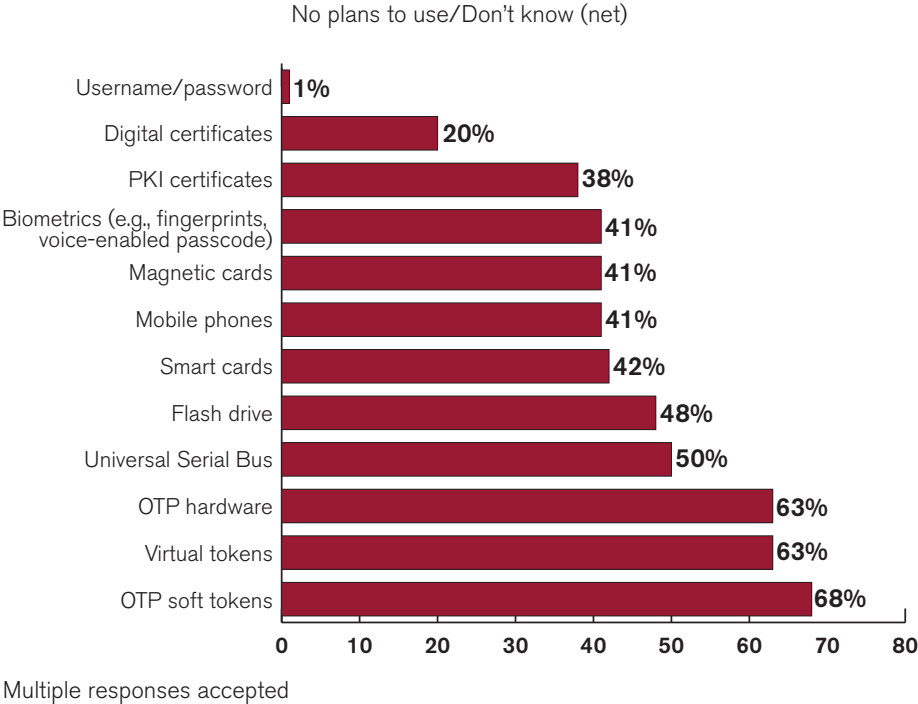


Have used in the past/Currently use (net)



Plan to use in next 12 months/Considering use in next 12–24 months (net)

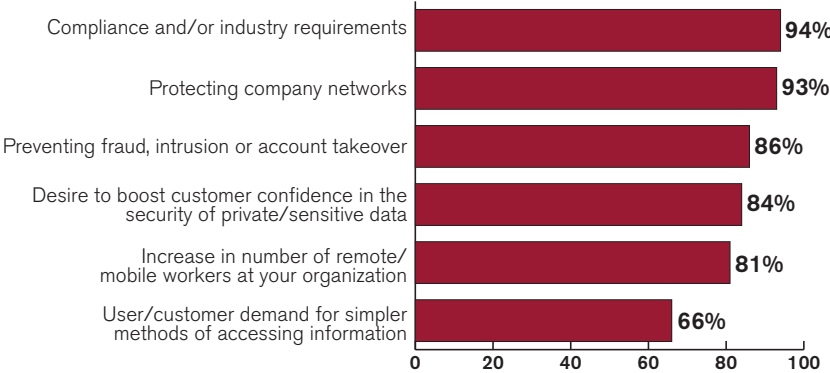




Effectiveness of authentication systems

Respondents rate their authentication system the highest for meeting compliance and/or industry requirements (94% rating very or somewhat well) and protection of their company networks (93%). However, there is more room for improvement in the following areas: preventing fraud, intrusion or account takeover (86%), desire to boost customer confidence in the security of private/sensitive data (84%), increase in the number of remote/mobile workers at their organization (81%), and especially user/customer demand for simpler methods of accessing information (66%).

How well does your authentication system address each of the following issues?

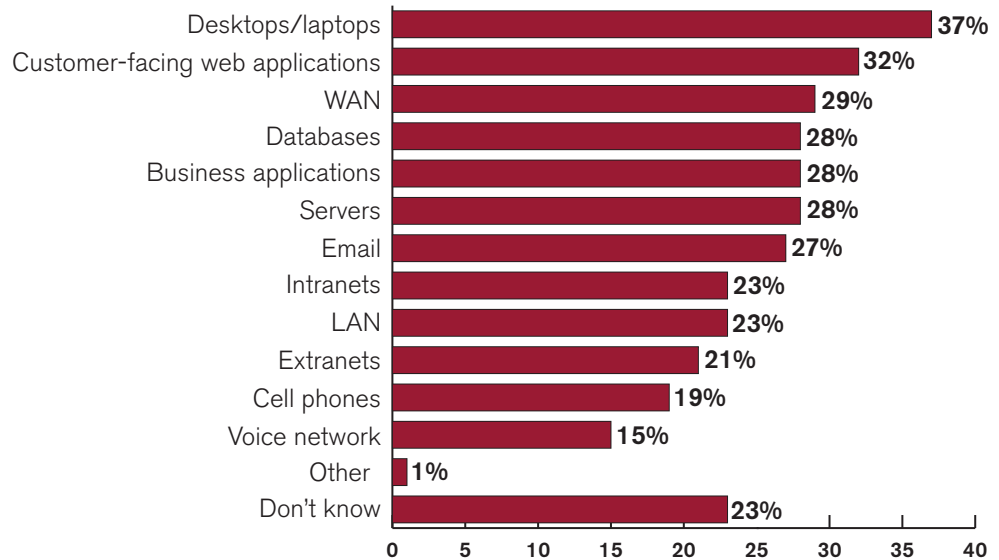


*Percentages represent respondents rating effectiveness for each factor as very or somewhat well

Areas for major changes to authentication systems

More than one-third of respondents (37%) expect to be making major changes to their authentication systems for desktops/laptops within the next 12 months. Other top areas for major changes within the next 12 months include customer-facing web applications (32%), WAN (29%), databases (28%), business applications (28%), servers (28%) and email (27%).

During the next 12 months, in which areas will your organization be making major changes to your authentication system?

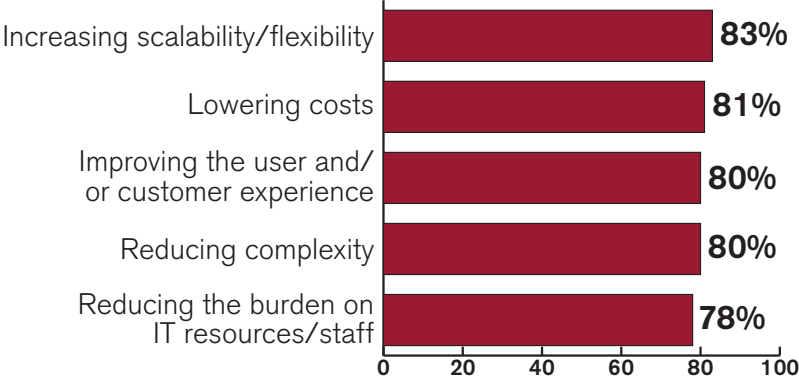


Multiple responses accepted

Important factors when evaluating an authentication solution

When evaluating an authentication solution to secure sensitive information, 83% of respondents rate increasing scalability and flexibility as a critical or very important factor. Not surprisingly in this economy, another factor respondents rate as critical or very important is the solution's ability to help lower costs (81%). Eight out of 10 respondents also rate the solution's capacity to improve the user and/or customer experience (80%) and reduce complexity (80%) as critical or very important when evaluating an authentication solution.

Please rate the importance of the following when your organization is evaluating an authentication solution to secure sensitive information.

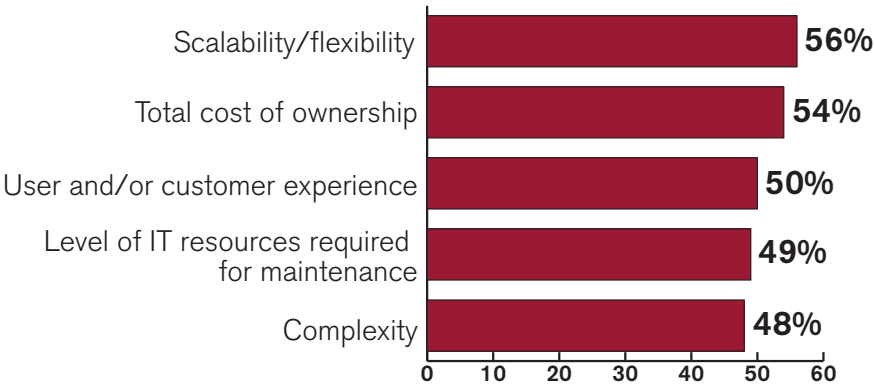


*Percentages represent those rating critical or very important for each factor

Performance of current authentication solutions

It is clear that there is room to improve in a number of areas related to authentication solutions, with just over half of all respondents (56%) rating their organizations' current authentication solutions' scalability/flexibility as excellent or good, and 54% noting this rating for total cost of ownership. Additionally, only half of respondents (50%) rate their authentication solutions as excellent or good for user and/or customer experience, while less than half of respondents rate their authentication solution as excellent or good for the level of IT resources required for maintenance (49%) and level of complexity (48%).

How would you rate your organization's current authentication solution(s) in the following areas?

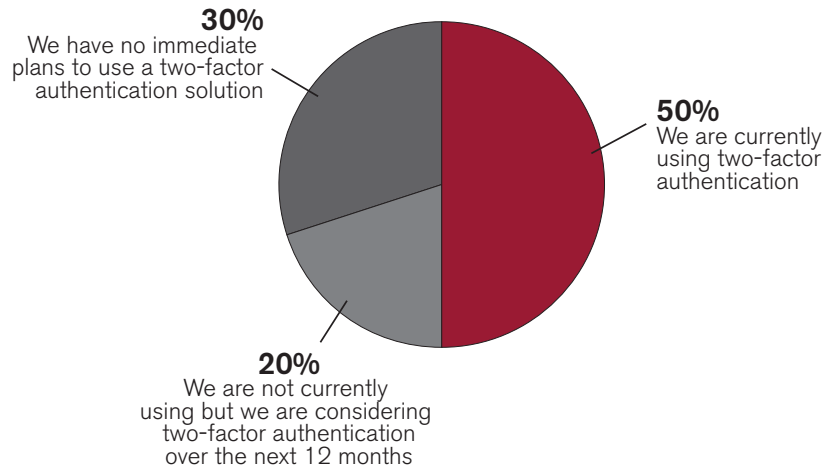


*Percentages represent those rating excellent or good for each area

Usage of two-factor authentication

Just half of respondents (50%) report that their organizations are currently using two-factor authentication. Only two out of 10 (20%) are considering two-factor authentication over the next 12 months and three out of 10 (30%) have no plans to use two-factor authentication.

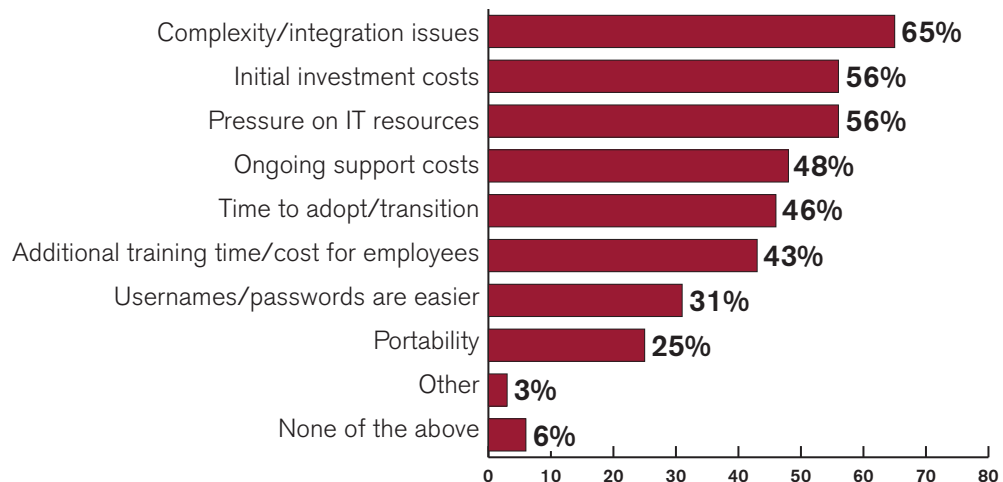
Based on the definition provided earlier in the survey, is your organization currently using or planning to use a two-factor authentication solution in order to control access to sensitive information?



Challenges of adopting two-factor authentication

Two-thirds of respondents (65%) are concerned with complexity and integration issues with the adoption of two-factor authentication. Over half find the initial investment costs (56%) and the pressure it would put on IT resources (56%) as barriers to adoption.

Regardless of your organization's plans regarding two-factor authentication, what challenges or barriers do you associate with the adoption of two-factor authentication?



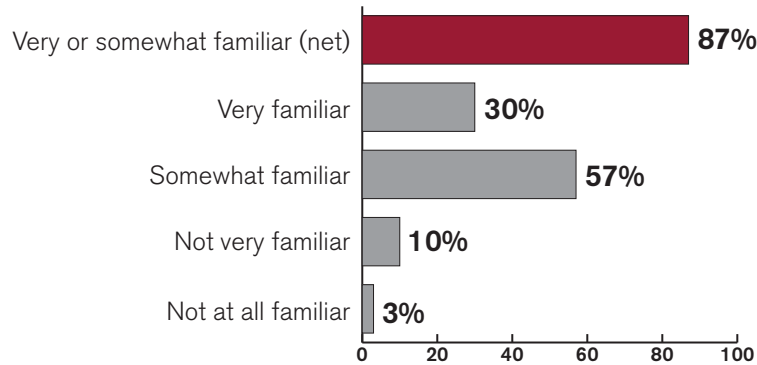
Multiple responses accepted

Familiarity with cloud computing

Based on the definition provided in the survey, almost nine out of 10 respondents (87%) are somewhat or very familiar with cloud computing.

For the purposes of this survey, “in the cloud services” are defined as a method of computing that uses a third-party service through the Internet for storage and management, thereby relying on shared computing resources versus local servers or personal devices to handle applications.

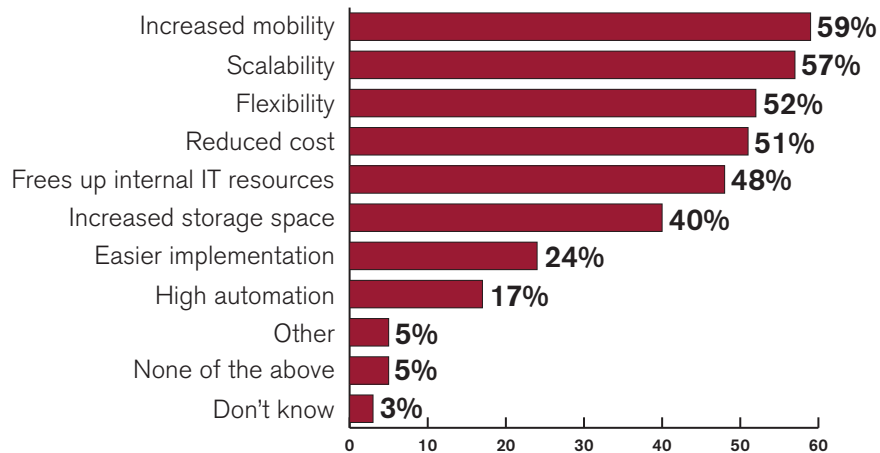
Based on the above definition, how familiar are you with cloud computing?



Potential benefits of cloud computing

Respondents most frequently cite increased mobility (59%) as a potential benefit associated with cloud computing. Other top benefits include scalability (57%), flexibility (52%), reduced cost (51%) and frees up internal IT resources (48%). Only 5% of respondents see no benefits associated with cloud computing.

Which of the following potential benefits do you associate with cloud computing?



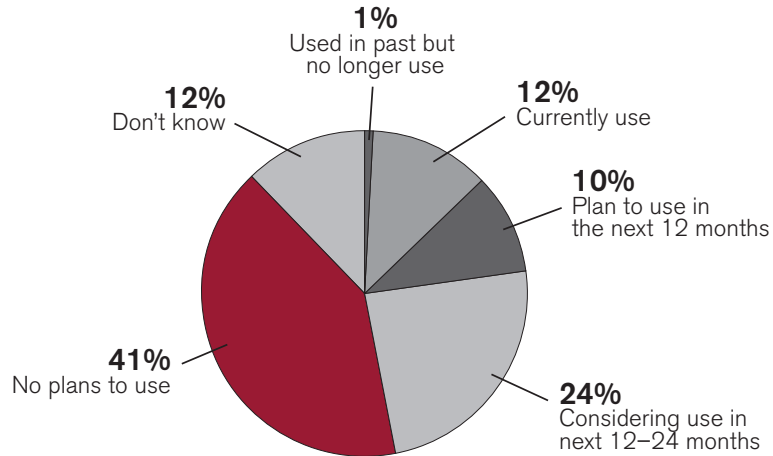
Base: 151 respondents who are familiar in some way with cloud computing

Multiple responses accepted

Adoption of cloud services for authentication systems

Only 13% of respondents have used or are currently using cloud services for their authentication systems (12% currently, 1% used in past). Ten percent (10%) have plans to use cloud for authentication within the next 12 months and almost one-quarter (24%) are considering cloud services for authentication within the next 12–24 months. Four out of 10 respondents (41%) have no plans to use cloud services for their authentication system.

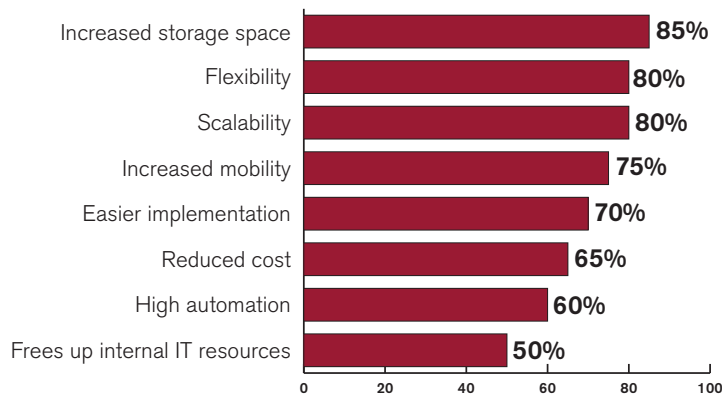
Which of the following most accurately describes your organization’s adoption status with regards to cloud services for your authentication system?



Experience with cloud computing

Respondents have had an excellent or good experience with cloud computing for the following factors: increased storage space (85%), flexibility (80%) and scalability (80%). Three-quarters of respondents (75%) indicate that they have had an excellent or good experience with cloud computing in regards to increased mobility, while 70% rate an excellent or good experience with easier implementation.

Please rate your organization’s experience with cloud computing in regard to each of the following factors.



Base: 20 respondents who currently use or have used cloud in the past

*Percentages represent those rating their experience as excellent/good for each factor

Conclusion

Two-factor authentication solutions provide an additional layer of protection for an organization's most sensitive data. While single layers and more vulnerable types of authentication factors, such as simple usernames and passwords, were once sufficient to authenticate a user's permission, those maliciously attempting to breach security measures have become increasingly sophisticated. As a result, organizations are finding that they need to exceed that sophistication with their security measures.

Respondents report that the important features of an authentication solution include the solution's scalability and flexibility, and the total cost of ownership for the product. Another important quality for an authentication solution is its ability to help reduce the burden on IT resources and staff. Interestingly, only 56% of respondents rate their current authentication solutions as excellent or good for any of the aforementioned important factors.

As with any change, respondents perceive that there are certain barriers or challenges inhibiting their adoption of two-factor authentication. Two of the frequently cited challenges, cost and pressure on IT resources, are closely aligned with the features that respondents report as important that any authentication solution under evaluation address. A way to overcome these challenges is to choose a provider that uses cloud computing for its authentication solution offerings. While most respondents are familiar with cloud services, only a small portion use cloud for authentication. Those who have used cloud with their authentication system frequently rate their experience with cloud as excellent or good, particularly for increasing storage space, scalability and increased mobility.

Two-factor authentication allows organizations to feel more confident that their data is secure, and to reduce the vulnerabilities created by today's remote and wireless work environment. The additional layer of protection makes security breaches more difficult by requiring two separate factors to validate identity. With the need for increased mobility, flexibility and scalability in security systems, while at the same time reducing overall costs and the burden on IT resources, organizations should turn to a vendor offering two-factor authentication solutions delivered in a cloud-based model with flexible choices of credentials that deliver cost and operational savings.