SafeNet | THE DATA PROTECTION COMPANY

Multi-factor Authentication

Current Usage and Trends

WHITEPAPER

Executive Summary

In this digital age, validating identities and controlling access is vital, which is why multi-factor authentication has become such a fundamental requirement in so many organisations. As security teams contend with cloud migrations, the influx of consumer devices, and other trends, the approaches, strategies, and plans for authentication will continue to evolve. This white paper draws on a large survey to provide a current picture of the authentication landscape in Europe, the Middle East, and Africa (EMEA), and it offers insights into how this landscape is expected to change in the coming years.

Introduction

Throughout EMEA, security teams have been relying on multi-factor authentication for quite some time. Today, however, the nature of authentication is changing in some fundamental ways:

- **Expanding usage.** Demand for authentication continues to grow. In the past, authentication was often deployed within an enterprise to address specific groups and use cases, such as VPN access. Now, there is a trend toward making authentication standard operating procedure for a much broader set of users and uses, such as safeguarding access to collaboration portals and cloud-based services.
- **Increasing urgency**. The need to leverage multi-factor authentication continues to grow increasingly urgent. This urgency is being driven both by traditional demands to mitigate risk and address compliance mandates, and to sustain security in the midst of such emerging trends as the adoption of cloud services, collaboration tools, and bring your own device (BYOD) mandates. For example, in cloud environments, multiple tiers and types of administrators may have access to infrastructure and assets, so leveraging multi-factor authentication to track and control this access is vital.
- **Evolving technology.** Given the shifts in the technological environment brought about by virtualisation and other advancements, the use of authentication continues to evolve. Additionally, the increased use of smart phones in an enterprise enables expanded use of multi-factor authentication, while complementing existing deployments.

To gain a better understanding of how the authentication landscape is evolving in EMEA, SafeNet conducted an extensive survey of senior IT and security professionals from across the region. This white paper reports on the findings of this research, providing a current look at the authentication market and some insights into where it is headed.

Top Survey Findings

- **Cost is the biggest inhibitor of more authentication adoption**, and the factor most likely to lead to a change in vendors.
- Authentication costs vary widely, with about **20% spending less than 15 euros per user a year, while 15% spend more than 48**.
- Cloud-based authentication appears to be gaining momentum, with **20% favorably inclined toward this approach.**
- Employee usage of authentication is expected to grow. The percentage of respondents that have **90-100% of employees using multi-factor authentication is expected to double in the next two years.**
- **Mobile authentication is on the rise**, and is expected to equal hardware-based deployments in two years.

Summary of Top Findings

While the survey revealed many significant findings, following is a summary of some of the most interesting:

- **Criticality of cost.** Survey respondents consistently pointed to cost as a significant factor. Cost was cited as the biggest inhibitor to more widespread authentication adoption, and as the factor that would be most likely to incent respondents to switch authentication vendors.
- **Costs run the gamut.** While there was clear consensus as to the significance and impact of cost, when it comes to spending levels, respondents reported a very diverse picture, with the number of respondents fairly evenly split across categories. For example, while 20.5% say they are spending less than 15 Euros per user annually, almost 10% say they spend more than 60 Euros.
- **Cloud-based authentication.** While server-based authentication represented the preference for the majority of respondents, already 20% prefer cloud-based authentication. At this early stage in the development of cloud authentication offerings, this represents a significant percentage.
- **Expanded employee usage anticipated.** Virtually all organisations are employing multi-factor authentication today, and across the board, adoption is expected to grow. Currently, 32.4% of respondents indicated that less than 10% of the workforce is using multi-factor authentication. Only 12% expect that to be the case in two years. In two years, 50% of respondents expect that at least half of all employees will be using two-factor authentication.
- **Anticipated rise in mobile authentication.** Currently, while rates of mobile authentication use are well behind hardware-based authentication, that is expected to change. Respondents indicate that mobile authentication will grow substantially, from 27.6% to 44.87%, in two years, at which point its rate of usage will be close to equaling that of hardware tokens.

In the sections that follow, we'll provide more details on these and other findings from the survey.

Two-factor Authentication: Employee Usage in the Enterprise

Several survey queries looked at the usage of two-factor authentication among employees, both currently as well as how that usage was expected to change in the future. Following is a breakdown of the areas these questions covered.

Employee Size of Respondent Organisations

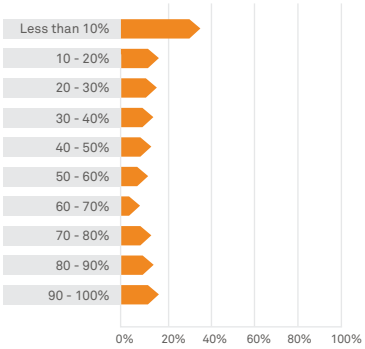
First, to provide some context on company size, the SafeNet survey gathered background on the number of employees within respondent organisations. Respondents came from a broad and fairly even mix of company sizes. About one quarter of respondents came from companies with less than 100 employees. A similar portion came from companies that have between 100 and 500 employees. 21% were from companies between 1000 and 5000 employees, and almost 17% came from companies with more than 5000 employees.

Current and Projected Footprint

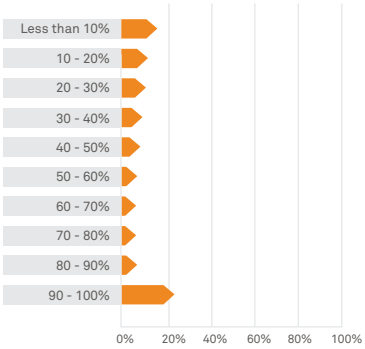
In general, there is plenty of room to expand employee usage of two-factor authentication, and it seems clear that's the direction for most organisations. Today, the biggest percentage, 32.4%, say less than 10% of the workforce is using two-factor authentication. On the other end of the spectrum, 12% say 90-100% of the workforce is. Otherwise, responses were pretty evenly split across the range of percentages.

The survey then asked respondents to estimate their authentication usage in two years. Only 12% said less than 10% of the workforce would be using two-factor authentication in two years, and 23% percent anticipated that 90-100% of the workforce would, which would represent almost a doubling of organisations with this level of authentication usage. In total, 30% of respondents indicated they have 50% or more of the workforce using two-factor authentication currently; 50% expect to achieve that number in two years.

Percentage of employees using two-factor authentication today



Percentage of employees that will use two factor authentication in two years time?



Overall, respondents expect more employees to be using multi-factor authentication, and the percent of those with 90-100% of employees using authentication is expected to double.

Inhibitors

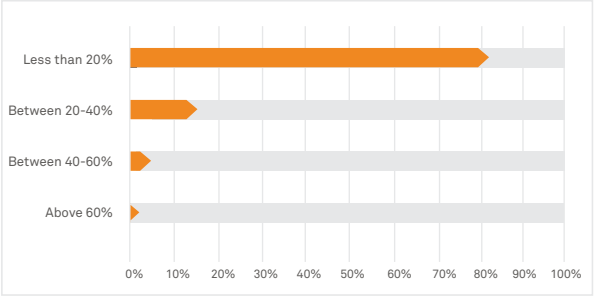
The survey also looked at what's keeping organisations from meeting that 100% level in terms of employee authentication usage. In short, it's a matter of money and time. 63% of respondents said cost would be the main barrier. 38.1% said time to implement and 34% said total cost of ownership.

Use of Multiple Tokens

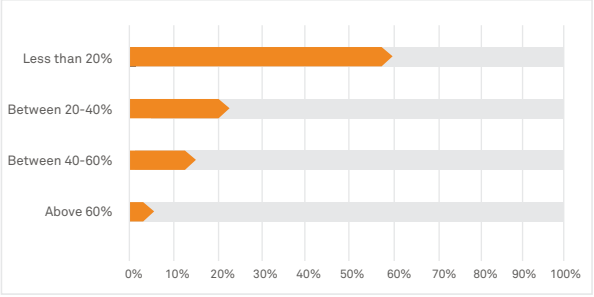
For many organisations, it is starting to make increasing sense to have employees use multiple tokens. For example, now one user may have a hardware token for desktop authentication, a software token for accessing corporate assets on an iPad, and an SMS token for using a mobile phone to access a business application. To get a picture of how common these scenarios are, the survey looked at the percentage of users in respondent organisations that need more than one token. 83% of respondents said less than 20% have more than one token. Only 17% have 20% or greater of the workforce using multiple tokens.

Respondents were also asked about how they expected the usage of multiple tokens to change in two years. A significant percentage, 57%, still say that less than 20% of employees will have multiple tokens. However, the number that expects more than 20% of employees to use multiple tokens grows from 17% to 42.3%. As organisations continue to expand the percentage of employees that use multiple tokens, it will grow increasingly critical to leverage a central authentication management platform that can support multiple, distinct device types. By doing so, companies can expand their token deployments, while minimising the corresponding increase in ownership and administration costs.

What Percentage of Users Use More than One Token



What percentage of users will use more than one token in two years



The number of employees using more than one token is expected to grow in most organisations, with four out of ten anticipating that 20% or more of employees will be using multiple tokens in two years.

Preferences: Server- vs. Cloud-based Authentication

The survey looked to gauge the preferences of respondents when it comes to choosing between authentication approaches based on cloud models and those based on traditional, physical servers. When asked to choose, almost 80% indicated they preferred server-based approaches, which seems to be a clear indication of preferences based on current experience and familiarity.

However, it is important to note that the 20.9% that indicated they preferred cloud-based approaches represents a significant number, particularly given the relatively recent advent of these alternatives. As a frame of reference, in a January 2012 report , Gartner had estimated that less than 10% of enterprises were implementing authentication in the cloud, and that they expected the number to grow to 50% by the year 2017. While it isn't possible to make direct comparisons across these different surveys, given the fact that the SafeNet survey, taken late in 2012, indicates 20% are now open to the cloud, it would appear momentum may be picking up in terms of cloud adoption, perhaps even faster than analysts anticipated.

Cost of Two-factor Authentication

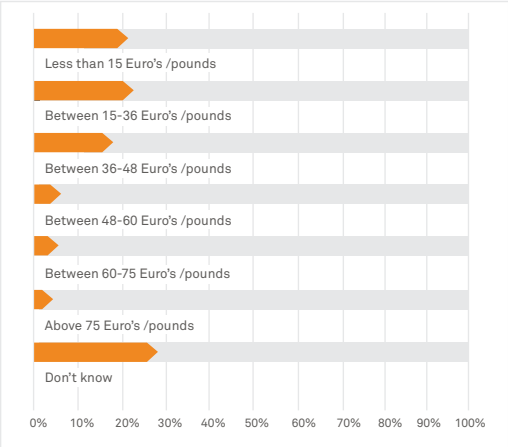
Costs play a major role in the nature and scope of authentication deployments in organisations, and in the plans for how these deployments will evolve. Consequently, the survey looked to assess costs in a few ways, asking respondents about current costs, the costs they expect to pay, and what they think they'll pay in two years. Note, the questions, and the statistics reported, all look at costs on an annual, per-user basis.

About 1/5th or 20.5% say they are spending less than 15 Euros currently. About the same percentage, 20.8% say they expect to pay less than 15 Euros in two years. However, 37.2% say they'd currently expect to pay less than 15 Euros. 22.9% currently spend between 15 and 36 Euros, and 36.7% say they'd expect to pay between 15 and 36. In two years, 30.98% expect to pay between 15 and 36. Thus, there seems to be a disconnect between what respondents pay currently and what they think they should be paying, but there's fair amount of consistency in that they expect costs to be fairly similar in two years.

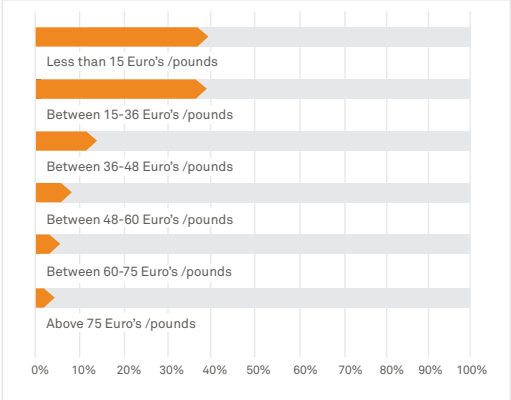
Also, it is interesting to note that 15.1% say they currently spend more than 48 Euros, with respondents fairly evenly split across three cost groupings: 48-60, 60-75, and over 75. Interestingly, about the same percentage, 13%, expect to pay more than 48 Euros. It appears that those who invest significant costs in authentication also expect to do so.

By reducing many of the costs associated with implementing and supporting an on-premise authentication infrastructure, cloud-based approaches offer the potential to fundamentally alter this cost picture, influencing both expenses and expectations. As more organizations move forward with cloud-based platforms, it will be interesting to track how these numbers change in the coming years.

Two-factor authentication solution cost per user per year: current costs



Two-factor authentication solution cost per user per year: expected costs



Currently, about 20% of respondents indicate they're paying less than 15 Euros, and about the same percentage anticipate that to be the case in two years.

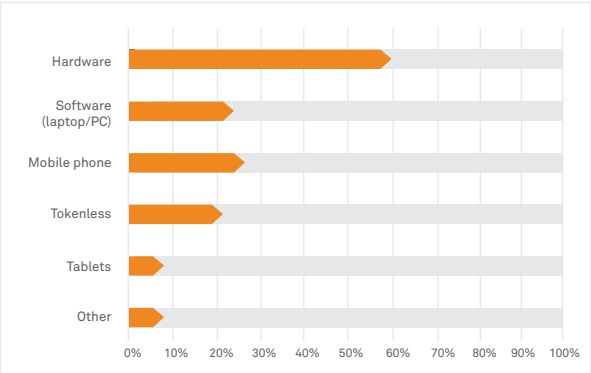
Token Types in Use

When asked about current usage of token types, respondents indicated that hardware tokens are the most commonly deployed, with more than 60% using these tokens. Currently, mobile phone-based tokens were second most common, receiving a response average of 27.6%.

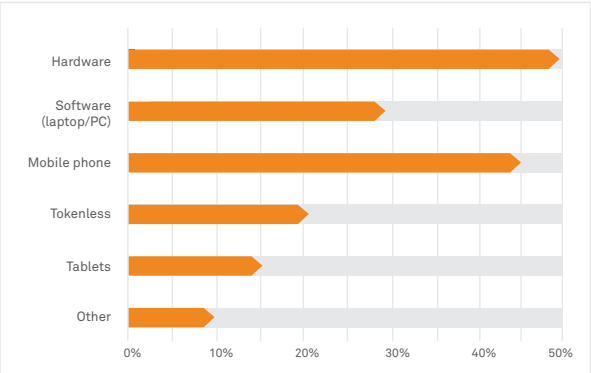
When asked to predict usage in two years, respondents see mobile phone token usage expanding, and hardware tokens declining, to the point where their usage is almost equal. In two years, respondents expect mobile usage to grow to 44.87%, while hardware usage is expected to drop to 48.89%.

Tablet-based tokens are expected to grow from 5.63% to 14.54%, while software based tokens are expected to remain relatively consistent: current usage is 26.81%, and usage is expected to grow slightly, to 29.08%. When totaling tablet and phone based authentication, the mobile authentication category will grow to almost 74%.

What percentage of users are using each type of token



What percentage of users are expected to use each type of token in two years

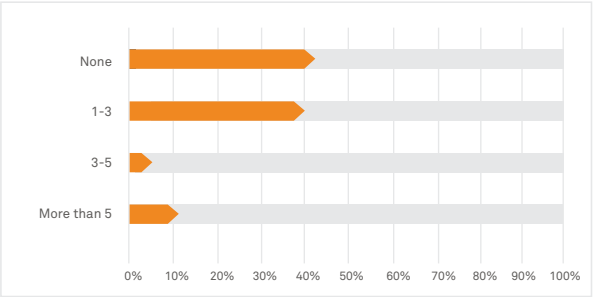


Currently, the dominant form factor, hardware token usage is expected to decline in the next two years.

Two-Factor Authentication: Applications

In many organisations today, two-factor authentication is predominantly being used for securing VPN access. When asked about the number of applications for which two-factor authentication is used other than VPN, 42% said none. 40.3% said they use two-factor authentication for one to three additional applications and 11.6% said they use it for more than five additional applications.

Apart from VPN, how many applications use two-factor authentication



Currently, over 40% of respondents are using multi-factor authentication for one to three applications, in addition to securing VPN access.

The survey also provided an open ended question as to the other applications for which two-factor authentication is being used. Following is a breakdown of the most common categories, and the relative percentage:

- Applications relating to authentication or access control (12.35%)
- Citrix applications, such as Citrix Web Interface, Citrix Web Access, and Citrix Access Gateway (11.5%)
- Banking, including financial applications and ebanking (11.11%)
- Webmail (9.88%)
- Business services and administration applications, including CRM and ERP (7.0%)

Authentication Vendors

The survey also explored respondent's views of their authentication vendors, looking at factors that would precipitate a change in vendors, and also the relative importance of professional services.

Factors that Would Precipitate Change

Given the fact that many felt cost was the biggest hindrance to broader adoption of two-factor authentication, it's not a surprise that cost would be a common justification cited for switching vendors. Following is an overview of the most common categories that responses fell into:

- 37.46% said cost
- 32.25% cited integration and usability
- 24.75% referenced security
- 5.86% pointed to reliability
- 2.28% either mentioned a breach of a specific vendor or alluded to the fact that a vendor breach or a loss in trust in the vendor was grounds to make a change

Importance of Professional Services

Respondents were asked to rate, when selecting a solution like two-factor authentication, how important it was that a vendor offer professional services. Respondents were given several choices, with options ranging from "not at all important" to "essential". Most respondents fell in the middle, with "important" receiving the highest response. Combining those who said "important", "very important", or "essential", the response adds up to 62.9%, indicating a majority find this a significant factor.

Key Implications and Planning Considerations

As the survey results detailed above make clear, in the coming years there looks sure to be a fair amount of flux in authentication approaches, uses, and deployments. As IT and security teams chart out how their organisations will navigate this evolving landscape in the next several years, there are a few key objectives to focus on:

- **Reduce costs.** For many organisations today, authentication exacts a high toll in costs, including lengthy, complex deployments, labor-intensive ongoing administration, and high volumes of calls into help desks, for example to field support for token requests. The survey amply illustrated how much of a barrier these costs are to more widespread adoption of authentication. To reduce costs, look for SaaS-based platforms that eliminate the need to deploy and support the hardware and software required to run authentication. In addition, look for platforms that automate authentication provisioning, service delivery, and reporting.
- **Maximise flexibility.** With the emergence of such trends as cloud services and BYOD, authentication approaches have had to evolve, and the pace of change shows no signs of slowing. Not only do organisations need to deploy authentication in more instances, but they need to have the flexibility required to support a broader range of use cases, risk profiles, and groups. Consequently, organisations should look for platforms that enable central management of the widest variety of token form factors, and that offer capabilities for tailoring deployments to specific user groups and assets.

- **Efficiently support mobility.** Within the next couple of years, mobile phone and tablet-based authentication is expected to be deployed in 74% of respondent organizations. To effectively and efficiently address this demand, security teams need to be able to support the provision of multiple tokens and multiple authentication methods for each user, according to the device or platform being used.
- **Ensure scalability.** As outlined earlier, the use of authentication is anticipated to grow in virtually every organisation. The platforms and approaches employed today will go a long way toward determining how effectively an organisation will be able to contend with these scalability demands in the coming years. As organisations look to invest in new authentication platforms, they should look for such capabilities as multi-tenancy, multiple language support, easy customisation to adapt to different use cases, and automation.

Conclusion

IT and security landscapes have been changing rapidly and dramatically in recent years, and organisations' authentication approaches are poised to undergo some similar transformations in response. For security professionals, we hope this paper provided an instructive look at where many of their peers are in this evolution, and how they are planning to proceed in the coming years.

About the Survey

This survey took place late in 2012, and is drawn from the responses of more than 500 survey participants. Respondents came from across EMEA, and represented a wide range of industries, including education, financial services, healthcare, high technology, manufacturing, and telecommunications.

About SafeNet

Founded in 1983, SafeNet, Inc. is one of the largest information security companies in the world, and is trusted to protect the most sensitive data for market-leading organisations around the globe. SafeNet's data-centric approach focuses on the protection of high value information throughout its lifecycle, from the data center to the cloud. More than 25,000 customers across commercial enterprises and government agencies trust SafeNet to protect and control access to sensitive data, manage risk, ensure compliance, and secure virtual and cloud environments.

Contact Us: For all office locations and contact information, please visit **www.safenet-inc.com**
Follow Us: www.safenet-inc.com/connected