2014 Authentication Survey
Executive Summary
How Organizations Are Responding to Mobile and Cloud Threats
Overview

As IT teams seek to keep sensitive assets safe, while supporting the evolving adoption of cloud-based services and BYOD, authentication mechanisms need to play an increasingly central role. How are organizations adapting their authentication approaches to contend with the changes and increased risks their businesses face? This executive summary reports on a recent survey to provide a look at the market, and where it's heading.

Authentication mechanisms play a central role in contending with all these changes and challenges, representing an increasingly critical instrument in the security team's toolkit. How are IT organizations adapting their authentication approaches to contend with all these changes? SafeNet recently completed a widespread survey to find out. Following is a summary of the top findings:

→ To address their increased exposure, including new gaps created by running applications in the cloud, organizations are growing more reliant on multi-factor authentication.

→ To contend with BYOD trends and the increasingly mobile nature of the workforce, usage of multi-factor authentication on mobile devices is rising.

→ To meet the growing demand for multi-factor authentication, while managing costs, IT organizations are increasingly looking to cloud-based authentication approaches.

"It's clear that many IT departments are locked in a perpetual battle, struggling to keep up with the rapid pace of technological change, while protecting the company against security risks. On one hand, almost every other week, we hear about a new attack or breach at a large enterprise. On the other hand, staff needs continuous access to corporate systems and applications to do their jobs. Quite simply, IT teams can't address their charters if they don't have secure, reliable authentication mechanisms in place."

Jason Hart, VP Cloud Solutions, SafeNet
Expanding Usage of Multi-factor Authentication

While the technical and security landscape is shifting fundamentally and quickly, one consistent theme is emerging: Multi-factor authentication will play an increasingly central role in an organization's security defenses.

In this year's survey, respondents were asked about current multi-factor authentication adoption and anticipated usage in two years. Combined with our 2013 survey, we have three data points to track adoption rates, and across the board, usage is rising.

The percentage of organizations with the majority of users employing multi-factor authentication is set to grow by 87%.

Businesses that have less than 10% of their workforce using multi-factor authentication is expected to decline by more than one-third.

Organizations with more than 90% of employees using multi-factor authentication should expand by more than 100%.
Increased Reliance on Multi-factor Authentication to Secure Mobile Access

There's a clear cause and a clear effect in today's authentication market. With more mobile devices being used to access corporate resources, there's a pervasive response: More mobile devices users are being required to use multi-factor authentication.

- Organizations that have more than half of mobile device users doing multi-factor authentication is expected to grow 60%.
- Businesses with less than 10% of users doing so shrinks by 60%.
- Companies with more than 90% of users relying on multi-factor authentication grows 50%.
Openness to Cloud-based Authentication

When it comes to authentication costs, there's already a broad disconnect between expectations and realities. For many respondents, actual prices are higher than they'd expect them to be. For example, while only 42% spend less than 36 Euros per user per year, 76% of respondents say they would expect to pay less than that amount.

Given the increasing usage of multi-factor authentication outlined above, it’s clear IT and security executives will have to balance the need to address this growing demand, while contending with ongoing budget pressures.

This realisation is a clear driver behind respondents’ increasing amenability to cloud-based authentication alternatives. Since last year’s survey, there’s been a 50% increase in respondents’ openness to cloud-based authentication.
Conclusion

In the authentication market, there's been plenty of change. In our survey, some clear patterns emerge. Most importantly, there will be more—more multi-factor authentication usage across the organization, and more usage from staff working on their mobile devices. These realities, coupled with the need to speed deployment and improve total cost of ownership, are clearly a big reason that cloud-based authentication, virtually an unknown a few years ago, is now the preference for more than 30% of respondents.

About the Survey

This white paper draws its findings from a survey of more than 350 individuals from around the world. About 29% were from the Asia Pacific region; 42% from Europe, Middle East, and Africa; and 29% from North America.

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 organizations 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.