



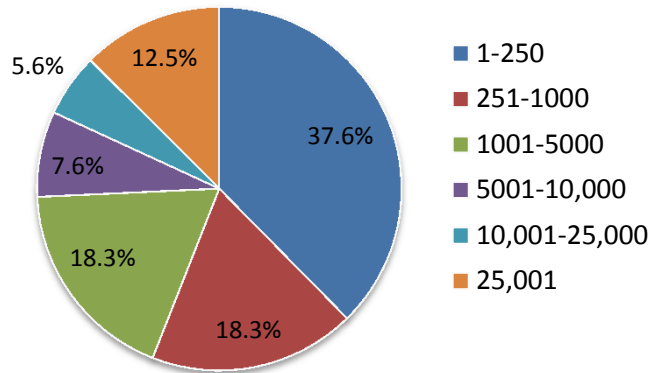
2011 Multi-Factor Authentication Survey:

Survey Reveals RSA Breach Undermining Confidence In Security Tokens

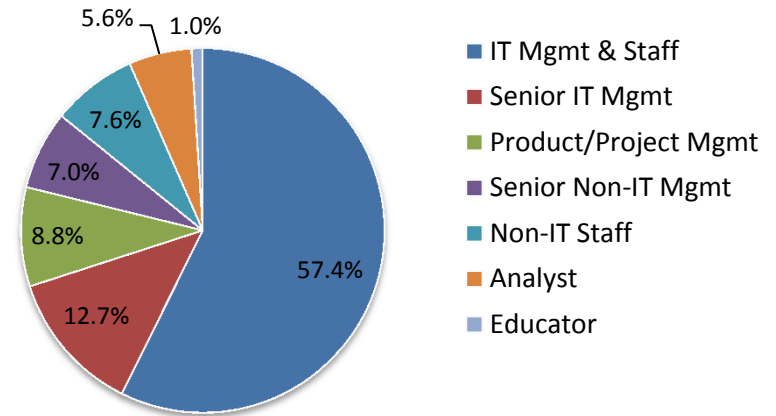
April 2011

PhoneFactor, Inc.

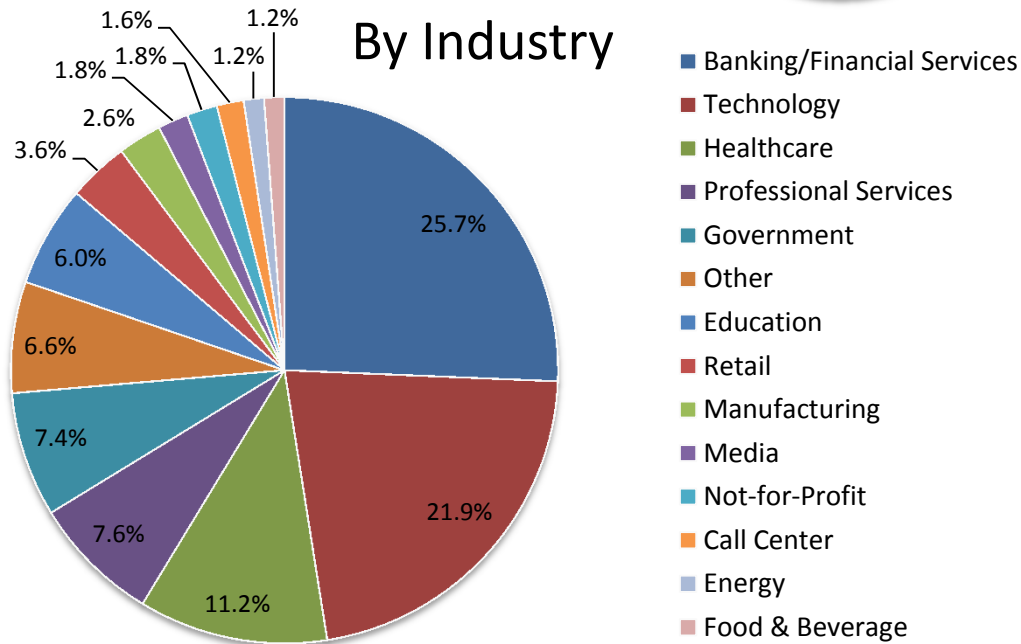
By Company Size (Employees)



By Role



By Industry



48.6% are currently using security tokens (hardware or software).

433 Respondents

Security Tokens Already Impacted By Security and Usability Issues



Those With Current Token Deployments

Of the 86% who are aware of these threats, **55%** indicated that recent man-in-the-middle threats have reduced their confidence in security tokens.

Q: Have man-in-the-middle or other recent threats, which defeat security tokens, reduced your level of confidence in the security provided by security tokens?



Those With Current Token Deployments

Of the 97% who are aware of the breach:

57% indicated that the RSA breach affecting SecurID has reduced their confidence in security tokens

44% indicated that the breach caused them to re-evaluate their use of security tokens

15% indicated that the breach caused them to speed up a current or planned review of alternatives

Q: Has the recent RSA breach, affecting SecurID tokens, reduced your level of confidence in the security provided by security tokens?

Q: Has the recent RSA breach impacted your organization's future use of security tokens?



Those With Current Token Deployments

If due to the RSA breach it became necessary to replace security tokens already deployed, **70%** of respondents would prefer to replace them with an alternate two-factor solution.

Q: If due to the RSA breach it becomes necessary to replace all of the security tokens deployed by your organization, which of the following would you prefer to do?

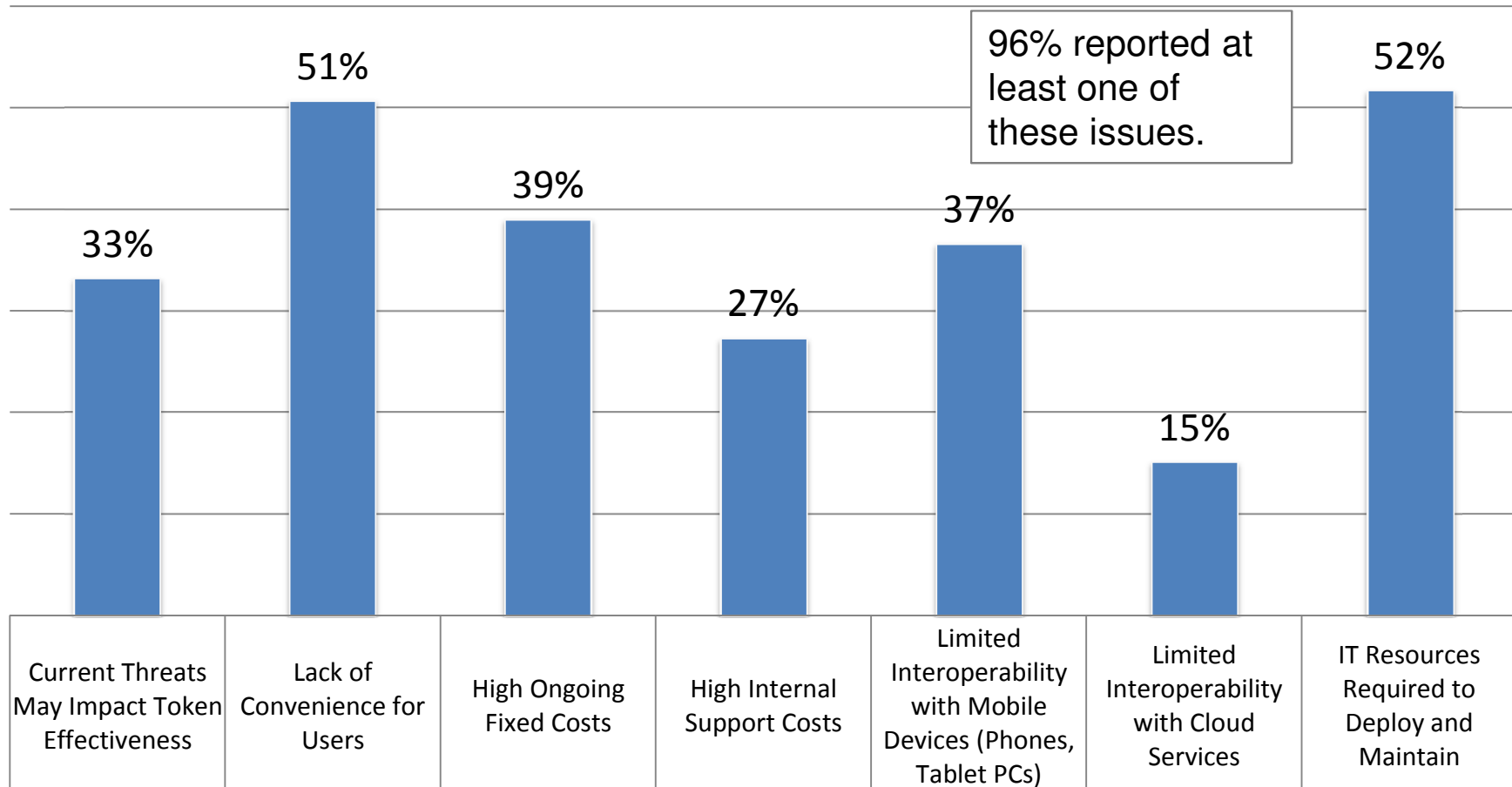


Those With Current Token Deployments

Due to security concerns related to tokens, **65%** of respondents are or will be evaluating the use of out-of-band authentication.

Q: Due to security concerns related to tokens, are you now or do you plan to evaluate the use out-of-band authentication?

Security Is Not The Only Area Of Concern

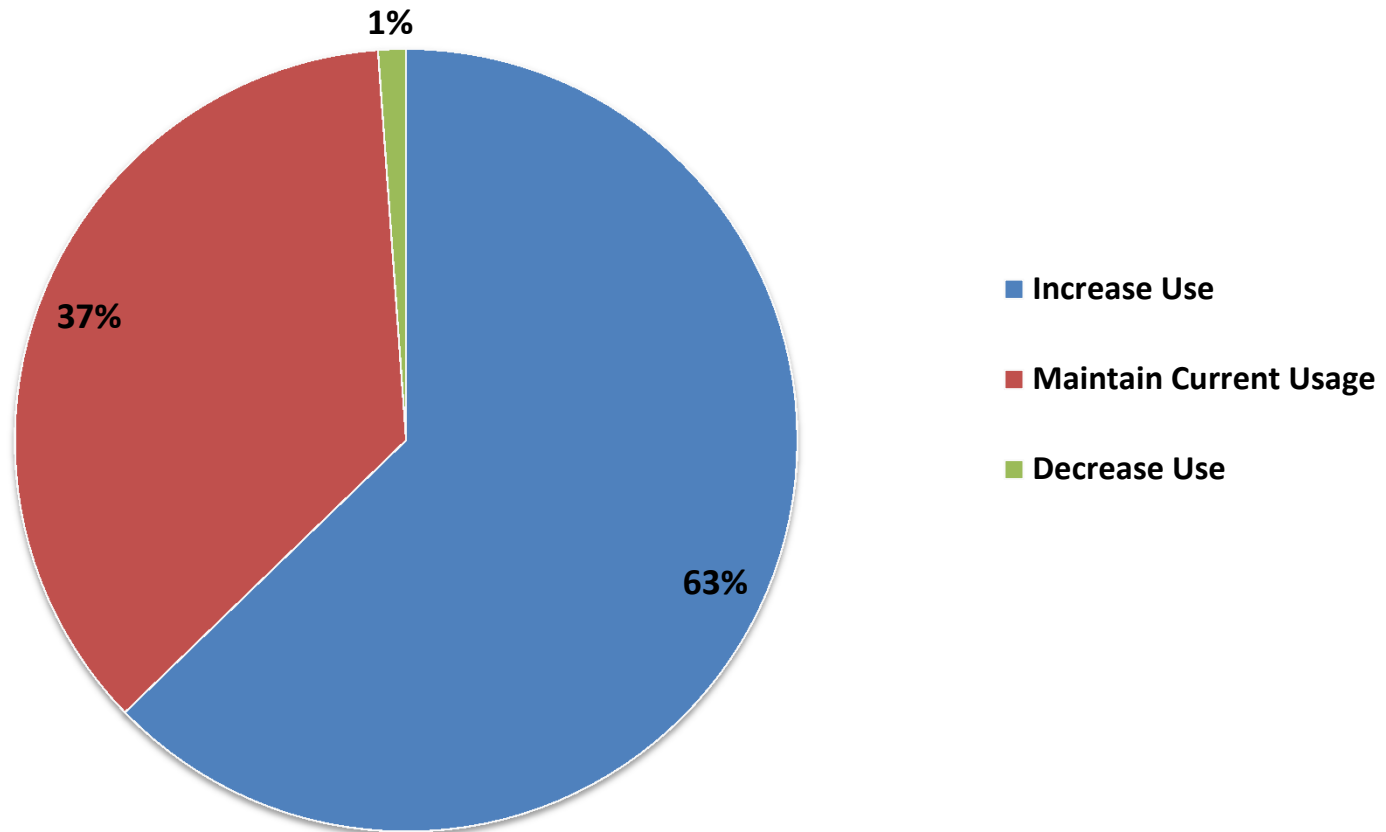


Q: Which, if any, of the following do you see as disadvantages to your organization's current use of security tokens? (Please check all that apply.)



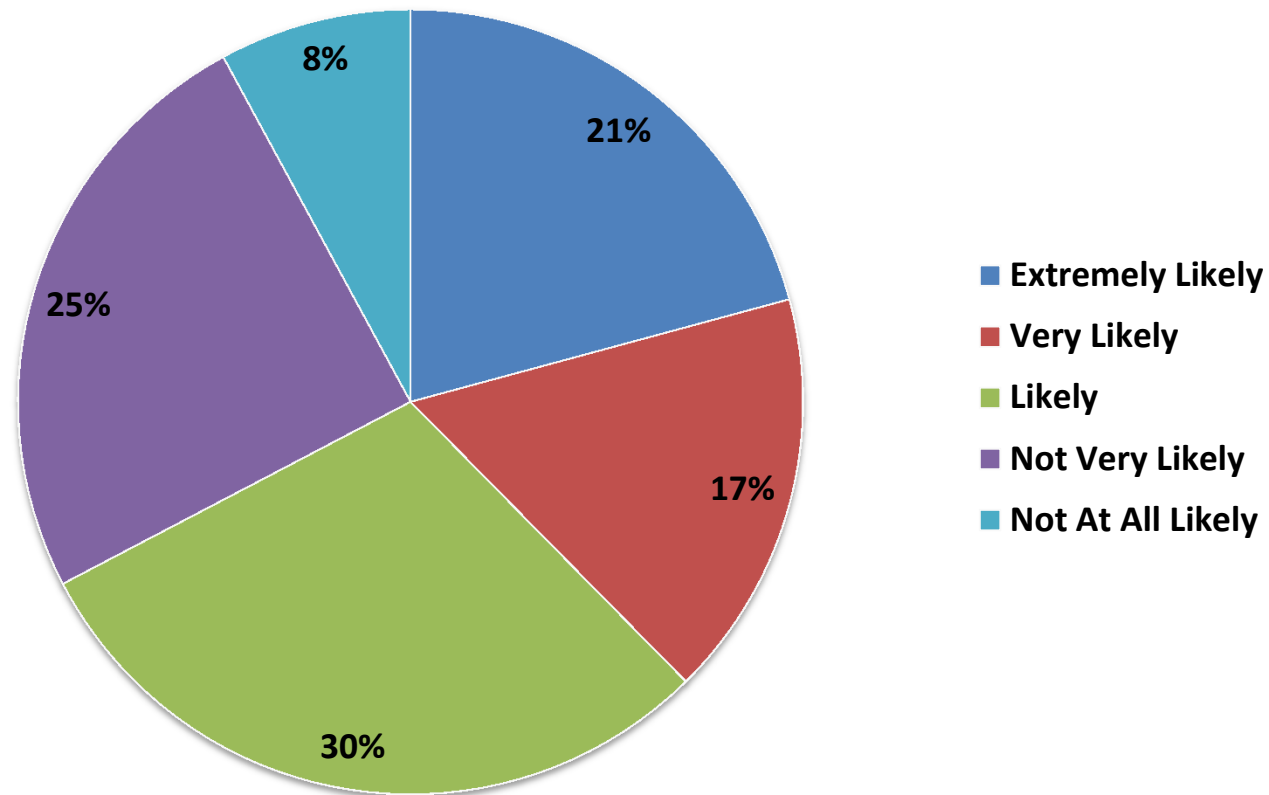
Organizations See Phone-Based Out-of-Band Authentication As A Leading Replacement

Use Of Alternate Two-Factor Methods Expected to Grow



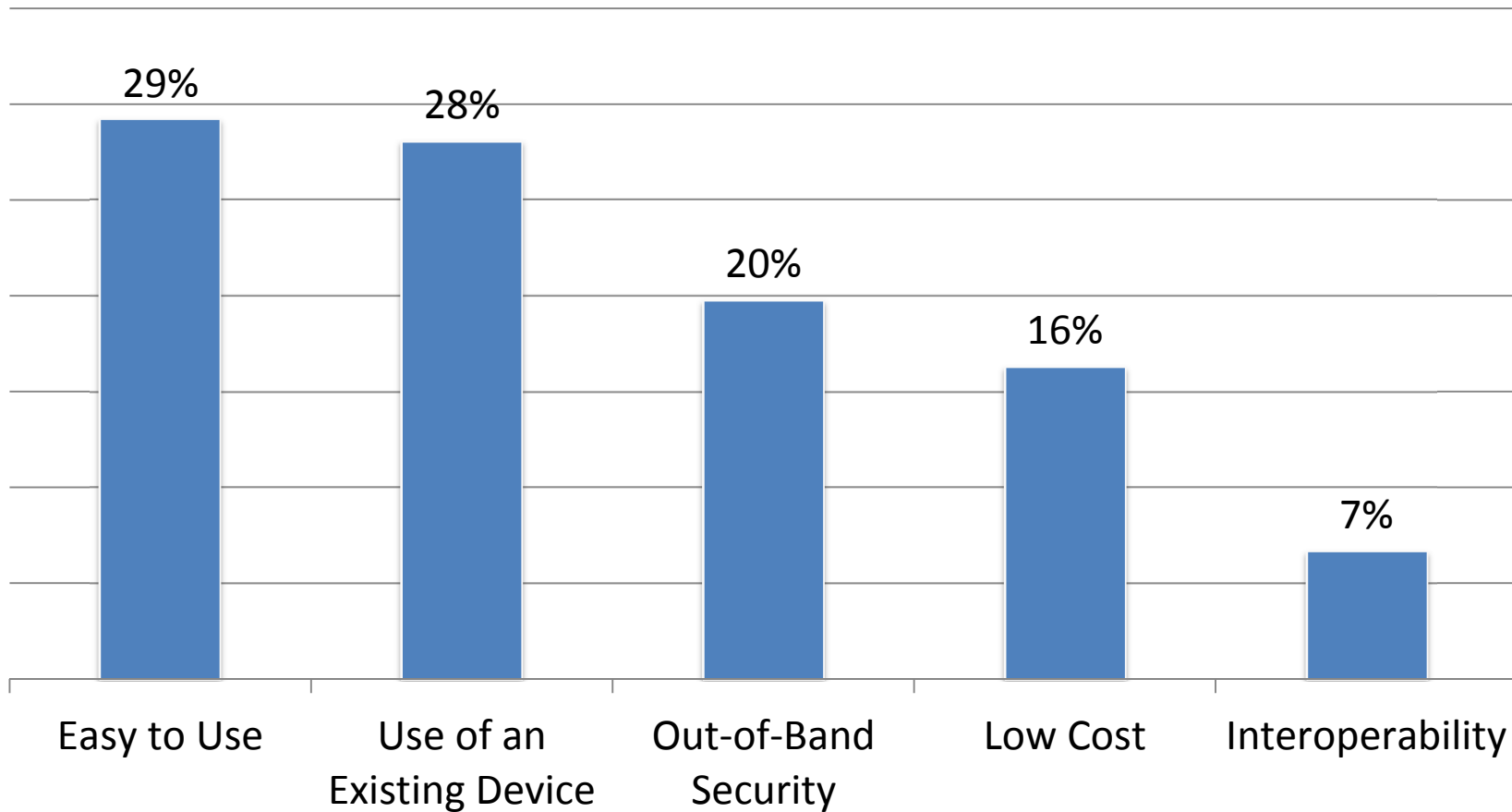
Q: With regard to your organization's use of OTHER two-factor methods over the next 2 years, do you plan to:

68% Are Likely To Use Phone-Based Authentication



Q: How likely is your organization to use phone-based authentication in the future?

Why Phone-Based Authentication



Q: What do you see as the primary benefit of phone-based authentication?

For banks, phone-based authentication is an even more popular alternative to tokens with:

81% evaluating the use of out-of-band authentication due to security concerns related to tokens (compared to 68% overall).

82% likely to use phone-based authentication (compared to 68% overall).

For banks, security is a stronger driver for the use of phone-based authentication:

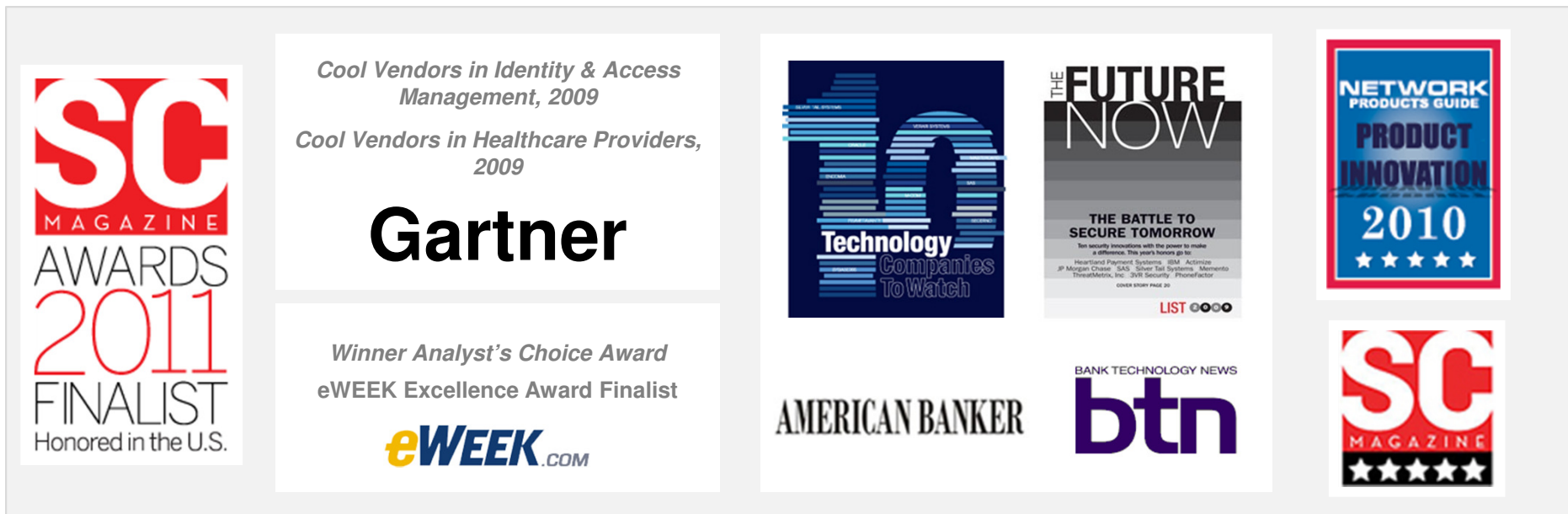
41% rated out-of-band security as the primary benefit of phone-based authentication (ease of use and use of an existing device were rated highest among respondents overall).



About PhoneFactor

PhoneFactor Is The Industry Leading Phone Authentication Provider

- Founded in 2001
- SAS 70 Type II Certified
- Recognition by Analysts and Press
- Award-Winning Platform
- Industry Leadership
- Trusted by Thousands of Organizations



Gartner Cool Vendors in Identity and Access Management, 2009 by Ant Allan et al. March 2009. Gartner's listing does not constitute an exhaustive list of vendors in any given technology area, but rather is designed to highlight interesting, new and innovative vendors, products and services. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness of a particular purpose. Gartner defines a cool vendor as a company that offers technologies or solutions that are: Innovative, enable users to do things they couldn't do before; Impactful, have, or will have, business impact (not just technology for the sake of technology); Intriguing, have caught Gartner's interest or curiosity in approximately the past six months.

Phone-Based Two-Factor Authentication

- No tokens for users to carry and track
- No software or certificates for end users to install
- No hardware or devices to purchase and manage
- Works with any phone, anywhere in the world
- No end user training is required
- Automated enrollment and user self-service
- Robust logging and reporting for auditing and compliance
- Out-of-band security
- Transaction verification capabilities



Two Easy Out-of-Band Authentication Methods

Step 1:

User logs into any application using their standard username and password.

Step 2:

Phone Call



*This is PhoneFactor.
Please press the #
sign to complete your
authentication.*

PhoneFactor places an automated phone call to the user. The user answers the phone and presses # (or enters a PIN) to authenticate.

SMS Text



PhoneFactor sends a OTP to the user in a text message. The user replies to the text message with the passcode (or the passcode and PIN) to authenticate.

Why PhoneFactor?

- **More Secure**
 - Out-of-Band authentication and fraud alerts offer unparalleled security.
 - Transaction verification protects against sophisticated attacks.
 - Biometric voiceprint adds a seamless third-factor of authentication.
- **Better User Experience**
 - Users do not have to carry and keep track of an extra device.
 - There are no software or certificates for end users to install.
 - In a recent client survey, 94% of users preferred PhoneFactor over security tokens.
- **Easier to Deploy and Support**
 - There are no hardware or software tokens to purchase, provision, manage, and support.
 - PhoneFactor enables rapid implementation, automated user enrollment, and requires very little ongoing maintenance.
- **Low Total Cost of Ownership**

BUSINESS IMPACTS

- **Decreased risk of a breach**
- **Regulatory compliance – PCI, HIPAA, NIST, etc.**
- **Reduced deployment time**
- **Decreased maintenance and support costs**
- **Increased employee productivity**
- **Significant savings over tokens and other two-factor solutions**