

Enterprise Readiness Series: The Case for Passive, Voice-Based Authentication

Today's customer authentication methods are from another age. Opus Research interviewed security and customer care professionals in Global 100 companies to learn about their perception and attitudes toward passive authentication of customers using voice. Respondents provided insights into the value of multi-factor authentication and provided "key success factors" for implementing strong, context-aware authentication without burdening customers with passwords or answers to challenge questions.

April 2013

Courtesy of:



Dan Miller, Senior Analyst – Conversational Commerce

Opus Research, Inc.
350 Brannan St., Suite 340
San Francisco, CA 94107

For sales inquiries please e-mail info@opusresearch.net or call +1(415) 904-7666

This report shall be used solely for internal information purposes. Reproduction of this report without prior written permission is forbidden. Access to this report is limited to the license terms agreed to originally and any changes must be agreed upon in writing. The information contained herein has been obtained from sources believed to be reliable. However, Opus Research, Inc. accepts no responsibility whatsoever for the content or legality of the report. Opus Research, Inc. disclaims all warranties as to the accuracy, completeness or adequacy of such information. Further, Opus Research, Inc. shall have no liability for errors, omissions or inadequacies in the information contained herein or interpretations thereof. The opinions expressed herein may not necessarily coincide with the opinions and viewpoints of Opus Research, Inc. and are subject to change without notice.

Published April 2013 © Opus Research, Inc. All rights reserved.

Table of Contents

Authentication: Stuck in the Last Century	1
Asking the Influencers	1
Pain Points with Current Authentication.....	1
Customers Really Don't Like the Authentication Process	2
Reliance on "Something You Know" Adds Time and Expense	2
Customers Have Too Much To Remember	2
Multi-Factor Authentication Drives More Complexity.....	3
Too Many Tokens, Dongles and Key Chains.....	3
Voice Biometrics Meets Today's Challenges	4
Ideal for Remote Authentication in the Voice Channel	4
Recap of Key Success Factors.....	4
Authentication Best Takes Place in the Background.....	4
Enrollment Has To Be Painless	4
Minimize Customer Effort in Enrollment and Authentication.....	5
Make It Multi-Factor	5
Deploy Risk-Based Authentication	5
Make it Customizable and Tune-able.....	6
Leverage Existing Infrastructure	6
Keep Innovating to Match Changing Threats	6
Convenient Security Becoming the Priority	7
How NICE Systems Addresses Authentication in Real Time	7
Case Made for Passive Voice Authentication.....	8
Appendix A: Factors for Authentication	9
Appendix B: Interview Guide	10

For a copy of the full report, please contact:

Pete Headrick

pheadrick@opusresearch.net

415-904-7666